NEWSLETTER

10-52

JUL 10

Support to Civil Authorities

Protecting the Homeland

Observations, Insights, and Lessons

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Newsletter. No. 10-52, July 2010. Support to Civil Authorities: Protecting the Homeland	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for Army Lessons Learned,10 Meade Ave., Bldg. 50,Fort Leavenworth,KS,66027-1350**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**138**	

Support to Civil Authorities: Protecting the Homeland Newsletter

Table of Contents

Center for Army Lessons Learned

Director	**Colonel Thomas Joseph Murphy**
Branch Chief	**Larry K. Hollars**
CALL Analyst	**William T. Smith**
Production Coordinator	**Joey Studnicka**
Editor	**Karen Blakeman**
Graphic Artist	**Eric Eck**
Distribution Manager	**Candice Miller**

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

Support to Civil Authorities: Protecting the Homeland

Introduction

The task of protecting borders and ports of entry from transnational and other threats to the security of the United States is a colossal undertaking, requiring the coordination and cooperation of many U.S. government agencies. This newsletter is a collection of articles, some previously published and other specifically written for this publication, that describe the critical nature of the homeland security mission, highlight some of the key agencies and organizations involved, and clarify the Department of Defense (DOD) role in providing support to this important task.

The line separating homeland defense from homeland security can be fine, but it is important to understand the differences between the two functions when examining the roles and responsibilities of agencies involved in detecting and deterring transnational threats. DOD is normally the lead agency for homeland defense, which is the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggressions and other threats as directed by the President. Homeland security, which is the focus of this newsletter, is a concerted national effort to prevent terrorist acts within the United States, reduce America's vulnerabilities to terrorism, minimize the damage from terrorism, and assist the population in recovering from attacks that do occur.[1] While homeland security is primarily the responsibility of civilian organizations and the National Guard working for the state governors, the military must be prepared to provide specific capabilities and make up for any shortfalls in extreme circumstances.

The first section of this newsletter provides a review of events since 9/11 that have shaped how the military prepares for and responds to homeland security events. It also discusses authorities and limitations and takes a look at the recently released 2010 Quadrennial Defense Review (QDR) as it applies to supporting civil authorities at home.

Border protection is a critical pillar of homeland security. It keeps dangerous people and materials out of the country and keeps terrorists from getting into position to attack.[2] The United States has approximately 7,612 miles of land boundaries and 19,924 miles of coastline in addition to the many seaports and airports through which international travelers and cargo pass each day. The second section of this newsletter looks at some of the initiatives in which DOD has supported other government agencies while protecting the borders and interdicting suspected transnational threats.

The third section examines the U.S. Coast Guard's (USCG's) role in providing maritime security to U.S. shores and seaports. The service's ports, waterways, and coastal security (PWCS) mission plays a key role in homeland security. Articles in this section enlighten readers on the mission and capabilities of the USCG as it protects the U.S. maritime domain and marine transportation system against attack, sabotage, espionage, and other subversive acts.

The nation's newest borders, which are neither land nor sea, may be the most vulnerable to transnational threats. Cyber borders protect our communications systems, financial and banking networks, and critical infrastructure. They also prevent electronic espionage and infiltration of DOD networks. The fourth and final section examines the threat of attack on our cyber borders and describes what is being done to protect them.

Defending our nation, at home and abroad, against foreign and domestic threats, is fundamental to the Army's legacy. When called upon, the roles of the military in protecting our borders may range from competencies that are not law-enforcement related, such as logistics, intelligence, surveillance, and communications, to the nonlethal tasks associated with supporting civil authorities in domestic contingencies. The intent of this newsletter is to stimulate thought, share ideas, understand the roles of the key agencies in protecting the borders, and examine how DOD provides support to the efforts of those agencies.

End Notes

1. Joint Publication 3-28, *Civil Support.* 14 Sept. 2007.

2. Testimony of Michael O'Hanlon, coauthor of *Protecting the Homeland 2006/2007,* 28 June 2006.

Section 1: Background

Securing America from Attack: The Defense Department's Evolving Role after 9/11

Frank L. Jones

Reprinted with permission from *U.S. Army War College Guide to National Security Issues.*

At 8:46 a.m. on September 11, 2001, a clear, sunny day on the East Coast, an American Airlines plane loaded with passengers, crew and thousands of gallons of fuel slammed into the 110-story north tower of World Trade Center in downtown Manhattan, exploding in a massive inferno. Seventeen minutes later, a second airplane, this time a United Airlines flight, crashed into the Center's twin south tower, igniting another firestorm. President George W. Bush, traveling in Florida, was informed of the incidents and immediately departed for the capital. Before leaving, he made a brief statement at 9:30 a.m. confirming that the planes were part of "an apparent terrorist attack" on the United States (U.S.). Less than 10 minutes after he spoke, a third airliner crashed into the U.S. Department of Defense (DoD) headquarters, more commonly known as the Pentagon, setting off an enormous fire causing hundreds of casualties; jet fuel literally ran down the corridors. The events did not end there. Shortly after 10:00 a.m., a fourth airliner plummeted to earth in a field just outside rural Shanksville, Pennsylvania, before it could reach its intended target, the result of a heroic effort by the passengers to prevent another horrific act from occurring.[1]

In a matter of less than 2 hours, both the World Trade Center's towers had collapsed, an unimaginable event, and nearly 3,000 people were killed. Manhattan was a storm of dust, ash, and debris. After the Pentagon attack, the Federal Aviation Administration, for the first time in U.S. history, shut down the nation's airspace, ordering all airborne planes to land immediately at the nearest airport. In their place, U.S. fighter jets streaked into the sky above the nation, their pilots ordered to shoot down any aircraft that did not comply. The horrific events of the morning now surpassed the nation's most famous day of infamy: the Japanese attack on Pearl Harbor 60 years earlier.[2]

The terrorist attacks were stunning not only in the tragedy they produced, but also as demonstrations of the creative lengths to which enemies of the United States could go to use everyday technology as weapons of mass destruction (WMD) against us. The capacity to wreck havoc of this magnitude was not unexpected for the signs of such an attempt had been foretold through a series of earlier events, both at home and overseas, including the 1993 World Trade Center bombing and an attack on the U.S. Navy destroyer *Cole* in Yemen in which dozens of crew members were killed or injured. What was startling to many Americans was the inability of the U.S. Government agencies to discern and prevent such a clever use of civilian aircraft. It was, as one of the commissions established to investigate the incident ominously warned, "a failure of imagination" on the part of the government.[3] These words also signaled that protecting the United States from further attack would be neither simple nor immediate despite the best intentions of U.S. Government leaders.

Years before the catastrophic events of September 11, 2001, various commissions established by the U.S. Congress urged the President and other officials to place substantial emphasis on improving the security of the U.S. against terrorist attack through increased resources, organizational redesign, and enhanced coordination among federal, state, and local governments.[4]

Unfortunately, September 11, 2001 would not only represent a distressing event in American history, it would take this tragedy to catalyze the governments and the private sector in the U.S. to undertake such a massive concerted effort to prevent such an attack from recurring. However, there was always the nagging realization that such an event could happen again, and if so, then the public and private sector needed to be prepared to respond to the consequences. Such an expectation had been noted decades before when President Calvin Coolidge gave voice to those fears in an address delivered before the American Legion convention in Omaha, Nebraska, on October 6, 1925. "In spite of all the arguments in favor of great military forces, no nation ever had an army large enough to guarantee it against attack in time of peace or to ensure victory in time of war."[5] Nonetheless, as the preamble to the U.S. Constitution underscores, it is the duty of the U.S. Government to "insure the domestic tranquility" and "provide for the common defense." Mindful of this obligation, U.S. Government leaders initiated a number of actions to respond to this exceedingly complex mission.

The attacks on the U.S. forced President George W. Bush and other administration officials to concentrate intently on the possibility of threats to the U.S. homeland. For DoD officials, there was recognition that the country had become, to use military parlance, a "battle space." There was an immediate refocusing from programs spending millions of dollars to develop a high-tech missile shield to prevent a ballistic missile attack by another state to fundamental concerns about a growing non-state threat. Thus, DoD would be given domestic duties to fight terrorism at home because as then Deputy Secretary of Defense Paul Wolfowitz explained, "The government is just not organized to deal with catastrophes on that scale, and when we do have catastrophes on that scale we inevitably end up turning to the military." There were skeptics nonetheless who contended that the military would embrace this mission as it would justify force structure and increase the defense budget, while Republican politicians would view it as an ironclad rationale for promoting national missile defense as a component of overall homeland defense.[6] More reflective thinkers recognized that defending the U.S. homeland against terrorism required a new paradigm—a new structure for meeting a more ambiguous challenge. The Pentagon no longer had to sell the idea of homeland defense politically. The issue now was how to make it work."[7]

The first response to this challenge was conventional with the president ordering a retaliatory strike on Afghanistan, which was harboring the Al-Qaeda terrorist leaders who had planned the suicide attack on Manhattan and Washington, and where this terrorist group had training camps. Nonetheless, there was no major overhaul of U.S. military forces nor was there a significant reallocation of funds to homeland defense missions, which had not even been defined. The 2001 Quadrennial Defense Review (QDR), presented to Congress in early October, largely upheld traditional thinking although it claimed that homeland defense was the Pentagon's highest priority. This document continued to stress U.S. advantages in space, information and power projection as well as the future of its nuclear arsenal. The underlying warfighting concept remained focused on combat with nation-states, emphasizing regime change in one war and repelling an aggressor in another.[8] One critic said the thinking remains "full speed ahead with the status quo," while Andrew Krepinevich, the executive director of the Center of Strategic and Budgetary Assessments, a Washington, DC think tank, complained that the QDR was a "thematic" document that called for transformation but provided no specifics on how this is to be accomplished. He was perplexed as to the Secretary of Defense's public statements that while the priority is on homeland defense, intelligence and other features for the changed strategic environment, new fighter jet programs remained the major acquisition programs.[9] Krepinevich's observation was astute. Although Rumsfeld heralded an ambitious program for transforming the military, the changes were marginal. The department had already begun to deflect any serious responsibility for this new mission by declaring in the QDR that the September 11 attacks

made clear that "the Department of Defense does not and cannot have the sole responsibility for homeland security." The only concession mentioned expressly was to consider establishing a new combatant commander for homeland defense.[10] In the White House, other actions were occurring at a more rapid pace. The President signed Executive Order 13228 on October 8, 2001, that established the post of Assistant to the President for Homeland Security in the Executive Office of the President as well as a Homeland Security Council, modeled on the National Security Council, which had existed since 1947.

The creation of this post and the council required Secretary of Defense Rumsfeld to name Secretary of the Army, Thomas E. White as DoD's first homeland security coordinator with responsibility for representing the department in council deliberations as well as interacting with the new homeland security advisor, a former Pennsylvania governor and member of the U.S. House of Representatives, Thomas J. Ridge. Pundits suggested that by naming White to the coordinator mission, the army would have a pivotal role in whatever responsibility is given to the military for homeland defense. White added to that perception by stating: "Since the early days of our nation, the army, both active and reserve, has engaged in homeland security. The army brings enormous experience, talent and capabilities to this effort."[11] The rhetoric was comforting to a nation still reeling from the attacks, but the exact role that White would have remained unclear. Nonetheless, Rumsfeld soon delivered on his promise to examine whether a separate combatant command should be established for the purpose of securing the U.S. homeland.

By mid-October 2001, a review of the Unified Command Plan was in progress. Rumsfeld was convinced that the current manner in which the armed forces were organized along regional lines was inappropriate to execute a global campaign against terrorism. There was considerable concern that transnational threats such as weapons proliferation and terrorism had not received sufficient attention from senior commanders and that the capability to coordinate with law enforcement concerning these threats from region to region was nonexistent. To fasten the military's attention on homeland defense there was also extensive discussion about the creation of an American command that would be responsible for the Western Hemisphere. In addition to this effort, the Pentagon leadership released the defense planning guidance for the war on terrorism that consisted of three goals: assail state support for terrorism, weaken its non-state support, and defend the U.S. homeland from additional terrorist attacks. Pentagon officials recognized that the current Unified Command Plan addressed the first two aims but not the third.[12]

By the end of 2001, Ridge and his staff were largely in place, but there were continued concerns by lawmakers and anti-terrorism experts that Congress needed to create a permanent homeland security post with a large staff and consolidate government agencies as part of it. The White House disagreed, arguing that Ridge could accomplish more as an adviser with the president's mandate and a staff detailed from other U.S. agencies than as head of a separate bureaucracy. DoD cautiously adopted its new homeland defense mission. By late January 2002, Defense officials sought to pull National Guard troops from security duties at the nation's airports, turning that responsibility over to the new Transportation Security Administration, which Congress established by law a month earlier. Approximately 6,000 troops were on duty at 400 airports across the U.S. to deter terrorists and reassure the public about the safety of air travel. The disengagement of the National Guard as a security force bespoke DoD's view that other federal agencies as well as state and local governments should handle the majority of the nation's homeland security duties. Ridge shared this view and declared that federal funding would be made available for this purpose. Secretary White endorsed Ridge's priorities, stating publicly

that the military should have a limited role in guarding the borders and policing airports and other potential terrorist targets in the U.S. Instead, it should concentrate on Afghanistan and other areas of the world. Additionally, National Guard troops assisting in border security in some states should be relieved of this duty also. Meanwhile, the DoD was considering scaling back the air patrols the Air Force had been conducting over major U.S. cities and critical infrastructure locations since September 11.[13]

White's remarks and the slow pace at which bureaucratic reorganization was occurring suggested to one observer, former U.S. ambassador and retired U.S. Army lieutenant general Edward Rowny, that there was a lack of urgency on the part of the Bush White House. Rumsfeld, however, in early February announced a proposal to establish a new regional command, Northern Command, to deal with the military component of homeland security. Rowny applauded Rumsfeld's initiative but contended that more needed to be done. He recommended that the Bush administration push for a similar consolidation and reorganization of the intelligence, border security, and emergency response agencies of the federal government. He also criticized Ridge's organization as ineffective because it lacked the needed tools and resources to handle a large-scale terrorist attack. Ridge, in Rowny's opinion, also had insufficient authority: he could not order federal agencies to act. Rowny's viewpoint was not a solitary one. Even the Bush administration recognized this deficiency, and in a speech at the National Press Club in Washington, DC, Ridge remarked that the President was considering reorganizing some federal departments and agencies, which would require congressional authorization.[14]

Meanwhile, Rumsfeld, sensing the mood of the country and particularly Congress, announced in April 2002, a military reorganization designed to give higher priority to homeland defense against terrorist attacks by the establishment of Northern Command. The new command, with headquarters in Colorado Springs, Colorado, and commanded by an Air Force general, was tasked to oversee the defense of U.S. territory, except for Hawaii and the U.S. possessions in the Pacific Ocean. Responsibility for these areas would belong to the existing U.S. Pacific Command. Northern Command would not only be responsible for the homeland defense mission, but would also coordinate with other federal agencies in preparing and responding to the consequences of a terrorist attack as well as natural and manmade disasters. Canada and Mexico would be included as part of the command's regional responsibilities.

Rumsfeld's decision was criticized, particularly by civil libertarians who were concerned about the use of the U.S. military for domestic security, particularly the erosion of constraints placed on the military by the Posse Comitatus Act. This federal law, enacted after the Reconstruction in 1878, prohibits the regular military from performing domestic law enforcement functions. Other critics expressed concern that the use of the military for domestic security and response diverted limited resources and weakened the military's effectiveness to fight wars overseas.[15] Almost simultaneously with the creation of the command, the Bush administration proposed the creation of a new executive branch department, the Department of Homeland Security (DHS).

Rumsfeld remained determined, however, to limit the scope of DoD's homeland defense mission. On May 7, 2002, testifying before the Senate Appropriations Committee, he continued to stress the importance of forward deterrence, that is, the prosecution of the war on terrorism abroad. Eventually, he turned to the subject of homeland defense and in doing so, articulated clearly and for the first time, the circumstances under which DoD would be involved in operations in the U.S. First, there were extraordinary circumstances that required DoD to execute its traditional military missions and therefore, DoD would take the lead with support from other federal agencies. Examples of these missions were combat air patrols and maritime defense operations. Also included in this category were cases in which the president, exercising his constitutional

authority as commander-in-chief and chief executive, authorizes military action. This inherent authority, Rumsfeld pointed out, may only be used in instances such as terrorist attacks, where normal measures were insufficient to execute federal functions. The second category was more traditional: in emergency circumstances of a catastrophic nature. Rumsfeld offered the example of responding to an attack or assisting other federal agencies with natural disasters. In these cases, the department would be providing capabilities that other agencies did not possess. The third category he described as missions limited in scope, where other agencies have the lead from the outset, giving the example of security at a special event such as the Olympics.[16]

Rumsfeld stressed that of the three categories, the first one was homeland defense since the department was carrying out its primary mission of defending the people and territory of the U.S. The other two categories were homeland security, whereby other federal agencies have the lead and DoD lends support. He continued by justifying the need for a $14 billion supplemental funding request for fiscal year 2002, and an increase in fiscal year 2003 funding of $48 billion. He added that both were essential for the war on terrorism but made no claim that any of the funding would be used for homeland defense. This was understandable given his limited definition of the department's role.[17]

He also announced that the president had approved a major revision of the Unified Command Plan and that one feature was the establishment of a combatant command for homeland defense, U.S. Northern Command at Peterson Air Force Base, Colorado. The primary missions of the new command were defending the United States against external threats, coordinating military support to civil authorities, as well as responsibility for security cooperation with Canada and Mexico.[18]

He followed this announcement with another, stating that he had established his own interim Office of Homeland Defense, and his intention to establish, by summer, a permanent office in the Office of the Secretary of Defense. The office would ensure internal coordination of DoD policy, provide guidance to Northern Command regarding homeland defense and support of civil authorities, and coordinate with the White House's Office of Homeland Security and other government agencies.[19]

Lastly, he assured the committee members that the department was conducting the study on the DoD role in homeland defense directed by the 2002 National Defense Authorization Act. Specifically, the comprehensive plan on how best to structure the Office of the Secretary of Defense to combat terrorism, defend the homeland, and enhance intelligence capabilities was expected to be completed during the summer.[20] The plan was completed as promised.

Acting on the recommendations in that plan, in July 2002, Rumsfeld decided to reorganize the Office of the Secretary of Defense by adding the position of Assistant Secretary of Defense for Homeland Defense based on the plan required by Congress. He selected Paul McHale, a former Democratic member of Congress from Pennsylvania, as the first to hold this position, pending Senate confirmation. One of the new assistant secretary's responsibilities would be to serve as a liaison between the Department of Defense and the proposed new homeland security department.[21]

Weeks later, Rumsfeld found himself, along with the Secretaries of State and Treasury, and the Attorney General, in the midst of the Bush Administration's controversial plan to establish a new homeland security department using all or parts of twenty-two existing agencies, a proposal that the President laid out in June. Rumsfeld and the other cabinet officials testified in support of the President's plan before the House Select Committee on Homeland Security. The plan faced

substantial opposition because the 12 committees in the House of Representatives that oversaw these agencies wanted to preserve their oversight responsibilities. Some standing committees of the House had already voted against provisions of the proposed legislation to create the department. The presence of the four cabinet heads before the select committee underscored not only the seriousness of the issue, but also the interdepartmental nature of the homeland security function and the domestic and international dimensions of the mission, ranging from border patrol and law enforcement to immigration and the issuance of visas.[22] As Attorney General John Ashcroft noted, "America's security requires a new approach, one nurtured by cooperation, collaboration, and coordination, not compartmentalization, one focused on a single, overarching goal—the prevention of terrorist attacks."[23]The emphasis on homeland defense remained more rhetoric than reality in DoD at least in terms of funds, procurement programs, and force structure changes. The Defense Planning Guidance, a document providing budgeting and planning guidance to DoD components, that Secretary Rumsfeld issued in May 2002, placed greater emphasis on the new strategic concept, "forward deterrence," that is, a commitment to attacking potential threats overseas. While the projection of U.S. forces over long distances to fight new adversaries made sense, the Defense Planning Guidance paid no attention to the support missions that the Department of Defense might have to provide federal, state, and local responders should a WMD, such as a nuclear, chemical, radiological, or biological device, be detonated in the United States. Instead, the emphasis was primarily on a global strike capability with added emphasis on overseas intelligence collection, covert special operations, unmanned air vehicles, cyber-warfare, hypersonic missiles, and the capacity to prevent an adversary from disrupting U.S. communications and intelligence assets in space and to strike underground targets.[24] This was a position Rumsfeld articulated publicly in a *Foreign Affairs* article that appeared that spring.[25]

This narrow perspective was expected to change because of two events. The first was that Northern Command became initially operational as an organization on October 1, 2002. The second event promised equally dramatic change, based on a provision in the 2003 Defense Authorization Act, which Congress passed in October 2002. The act authorized the establishment of the position of the Assistant Secretary of Defense for Homeland Defense. Four months later, in February 2003, Paul McHale was confirmed as the first person to hold this position. Additionally, Congress established the new Department of Homeland Security by the Homeland Security Act of 2002, enacted in November. Its first secretary would be Tom Ridge. The only major provision of the law that affected DoD was that the Homeland Security Council was established statutorily, consisting of the President, Vice President, Attorney General, the Secretary of Defense and the newly created Secretary of Homeland Security.

In February 2003, the new department and the two new DoD organizations would faced the first test of their abilities to respond to a domestic event and coordinate with other U.S. Government organizations when the space shuttle Columbia broke up over Texas during reentry to earth. Within an hour after the disaster, Ridge conferred with intelligence and White House officials as well as Northern Command, and determined that the incident had not resulted from terrorism. Ridge put the Federal Emergency Management Agency (FEMA), now part of DHS, in charge of recovering debris from the shuttle, while Secretary Rumsfeld assigned Northern Command to assist with this effort; a variety of aircraft and ships responded.[26]

This experience also helped prompt a new presidential directive, Homeland Security Presidential Directive-5, Management of Domestic Incidents, in which DoD would ultimately have a substantial role in implementation. In this document, the President designated the Secretary of Homeland Security as the principal federal officer for domestic incident management. The Secretary of Defense was tasked to provide military support to civil authorities for domestic

incidents under the president's direction or when consistent with military readiness, the appropriate circumstances, and law. The directive indicated that even during these events, military forces would remain under the command and control of the Secretary of Defense. The Secretary of Defense and the Secretary of Homeland Security were to develop mechanisms to promote cooperation and coordination between the two departments. Lastly, the directive called for the formulation of a National Response Plan (NRP) that would integrate the federal government's domestic prevention, preparedness, response, and recovery plans into a single all-hazards plan. An initial version of the NRP was due to the Assistant to the President for Homeland Security by April 1, 2003, along with a recommendation for the time needed to develop and implement a final version of this plan.[27]

By the beginning of April 2003, with U.S. military forces having invaded Iraq a month earlier, and now within 50 miles of Baghdad, Rumsfeld's view about homeland defense was apparent: the best way to secure the United States was to pursue terrorists in their havens.[28] Meanwhile, Paul McHale was busily putting his office in place with all the attendant bureaucratic headaches associated with such a venture. He also had his first appearance before Congress in April, when he testified before the Senate Armed Services Committee regarding defense of the U.S. homeland. McHale reiterated Rumsfeld's three conditions under which the Department of Defense would be involved in activities within the United States. However, these conditions were already being eroded. As McHale indicated, since September 11, 2001, DoD had flown more than 28,000 sorties over U.S. cities and responded to more than 1,000 requests from the Federal Aviation Administration to intercept potential air threats. Air patrols over the U.S. domestic airspace were no longer extraordinary but routine.[29]

During the summer of 2003, McHale's office would devote substantial time to a major department-wide, Secretary of Defense-directed classified study of the homeland defense mission and the force structure required to execute that mission. Later that year, the office would shape the next Strategic Planning Guidance, which required his office to formulate with assistance from other DoD components a homeland defense strategy within a year.

On December 17, 2003, President Bush approved two new homeland security directives that affected DoD. The first document, Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization and Protection, established national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from attack. The directive recognized that there were several critical infrastructure sectors, each with its own characteristics and operating processes. Although the DHS would have principal responsibility for implementing this directive, specific departments were designated responsible for collaborating with business and industry, conducting or facilitating vulnerability assessments, and encouraging risk management activities to protect against terrorist attacks or mitigate their effects. The Department of Defense assumed responsibility for the defense industrial base, thereby gaining another homeland security mission.[30]

The President also issued Homeland Security Presidential Directive-8, National Preparedness, that established policies to bolster the preparedness of the United States to prevent or respond to threatened or actual terrorist attacks, major disasters, and other emergencies. This measure called for the establishment of a national all-hazards preparedness goal, mechanisms for improving the delivery of federal preparedness assistance to state and local governments, and defining actions to improve preparedness at all levels of government. The Department of Defense's role, though

not as major as other federal departments and agencies, was to provide the DHS with information concerning organizations and functions that could be utilized to support civil authorities during a domestic crisis.[31]

Despite the attention to these strategic issues, the tyranny of daily operational demands was also present. During the Christmas holiday season, intelligence indicators stressed that al Qaeda's intent to carry out multiple catastrophic attacks in the United States was greater than at any point since September 11. The indicators suggested that the terrorist group was testing the vulnerabilities of the air transportation system, both passenger and cargo. In response, Secretary Ridge announced an upgrade in the threat level from elevated risk to high risk or orange alert, the second highest level in the color-coded system, after President Bush approved the recommendation by Ridge along with senior officials of the Federal Bureau of Investigation, the Central Intelligence Agency, DoD, the Justice Department, and White House staff. Raising the threat level increased security measures across the country to protect government buildings, critical infrastructure, shopping malls and other places where large numbers of people congregate. This decision was not made lightly. A few months earlier, in response to al Qaeda suicide bombings in Saudi Arabia and Morocco, and after several orange alerts within a few months, Ridge and Rumsfeld opposed raising alert levels. Ridge argued that frequent changes only caused considerable psychological unease in Americans as well as making the public cynical. Rumsfeld stated that raising the alert diverted military resources from Iraq and Afghanistan.[32] The holiday season ended uneventfully, but operational concerns continued to intrude because of the need to refine security procedures.

Slowly and subtly, the three conditions for DoD involved in domestic activities that Rumsfeld articulated 2 years earlier were jettisoned. In March 2004, McHale appeared before the Senate Armed Services Committee to update the members on DoD's ongoing homeland defense initiatives. At that time he did not mention the three conditions. Instead, McHale laid out a concept of layered defense, which he called the lines of defense. The first line of defense was combating terrorism far from U.S. territory. The second line of defense was the air and maritime approaches to the United States and interdicting terrorists before they reached U.S. borders, which was largely the responsibility of two combatant commands—Northern Command and Pacific Command. Within the United States, the domestic law enforcement community was responsible for countering terrorist attacks, in a sense a third line of defense, with DoD ready to provide its capabilities to civil authorities, consistent with U.S. law. However, McHale also stated that DoD had established and maintained a small number of reaction forces in the United States. These forces consisted of U.S. Army and Marine Corps personnel who were postured to respond to a full range of threats if ordered by the president, and when deployed, under NORTHCOM's command and control.[33]

Additionally, throughout 2004, as had been the case in 2003, DoD actively continued to enhance its homeland defense and civil support missions. It maintained the readiness of its own forces by hosting exercises and participating in those sponsored by other government entities. Further, it was implementing its responsibilities under HSPD-7 regarding critical infrastructure by consolidating funding for this effort under a single program and managing it by a program office. It also undertook a number of supporting missions including establishing a DoD presence in the DHS's Operations Center, detailing personnel to DHS to fill critical specialties primarily in intelligence analysis and communication, creating various liaison mechanisms, and identifying and transferring technology items and equipment that DoD had or was developing that might be of assistance to federal, state and local governments in their homeland security roles. Simultaneously, the department was responding to requests for assistance from several civilian agencies—for example, providing emergency support in natural disasters such as Hurricane

Isabel and California wildfires. It also responded to the ricin incident on Capitol Hill in January 2005. That incident saw the first operational use of NORTHCOM's Joint Force Headquarters-National Capital Region, which provided the command and control of the U.S. Marine Corps Chemical-Biological Response Force's assistance to the U.S. Capitol Police. [34]

DoD support to the interagency was broadened in August 2004, when President Bush established by executive order, the National Counterterrorism Center under the direction and control of the Director of Central Intelligence. The primary function of the center was to serve as the hub for analyzing and integrating all intelligence pertaining to terrorism, except purely domestic intelligence information. Additionally, it was to conduct strategic operational planning for counterterrorism activities by integrating all the national instruments of power.[35] To that end, DoD, as well as other partner organizations, provided personnel to assist the center with its mission.

DoD also assumed a major role in the development of the National Response Plan (NRP) required by HSPD-5. The development of the initial NRP met with resistance from state, local and tribal governments as well as non-governmental organizations, since they were not consulted by DHS during its formulation. Consequently, DHS and a small group of its federal partners, including DoD personnel, began anew—mindful of outreach to other stakeholders—in an intense writing process of monumental proportions that addressed planning assumptions and considerations, roles and responsibilities of the variety of organizations involved in responding to an emergency, and a concept of operations. The NRP identified fourteen emergency support functions, of which DoD (U.S. Army Corps of Engineers) would have the lead for public works and engineering, but would be a supporting agency in the remaining 13. The document also included special support annexes dealing with myriad topics such as tribal relations and private sector coordination and incident annexes for specifically troublesome situations such as a terrorism event involving a biological agent or hazardous materials pollution.[36]

The document, consisting of more than 300 pages, was approved in December 2004 by Secretary Ridge along with 27 federal departments and agencies, the U.S. Postal Service, the American Red Cross, the Corporation for National and Community Service, and the National Voluntary Organizations Active in Disaster.

Within days of the NRP's approval, President Bush issued a combined National and Homeland security directive on maritime security, an initiative of his new homeland security adviser, Frances Fragos Townsend. This directive not only established U.S. policy regarding protection of the nation's maritime interests, but directed the development of a national strategy for maritime security and eight national plans addressing such critical subjects as the U.S. Government's capability to respond to a maritime threat, the nation's capacity to recover from an attack or disaster affecting the maritime infrastructure, and security of both the maritime transportation system and the related supply chain. The President tasked DoD and DHS to lead an interagency task force to formulate the national strategy for maritime security for his approval within six months. The eight plans were to be delivered nearly simultaneously.[37] This approach was fraught with problems since the plans relied on the guidance framed in the strategy as well as coordination with various state and local governments, transportation and port authorities, and maritime industry trade associations.

It turned out that maritime security was not the only domain that required additional attention. In May 2005, a privately owned Cessna 150 airplane inadvertently penetrated the 16-mile-radius no fly zone around Washington, DC, established after the events of September 11, and designed to prevent air attacks on the White House and the Capitol. Federal Aviation Administration

and DHS officials could not communicate with the pilot, so Secretary Rumsfeld gave military officials the authority to shoot the plane down, if necessary. Aircraft from DHS Customs and Border Protection and military fighters moved to intercept the plane, and after eleven tense minutes, the pilot heeded instructions to turn away from the city. The incident required Defense Department and civilian officials to review the effectiveness of the air defense system for the nation's capital. Once again, DoD and its civilian counterparts were confronting sensitive issues involving internal governmental decision-making, communications, and federal interagency relations as well as authorities.[38] With respect to the latter, the DHS, under the new leadership of Secretary Michael Chertoff, a former federal judge, argued that his agency should have the shoot down authority. President Bush rejected this request. Nonetheless, the incident led to increased congressional scrutiny of the procedures and agency responsiveness. The event was also a warning signal that although air transportation security had been upgraded, the focus had been limited to scrutiny of passengers and cargo security. However, the Homeland Security Council staff contended that this issue would have to be deferred since other areas such as domestic nuclear attention had priority.

A month earlier, President Bush issued another combined NSPD/HSPD, designed to enhance protection against an attack in the United States using a nuclear or radiological device, and to advance the technology and integration of detection capabilities among across federal, state, local and tribal governments. To achieve these policy goals, the chief executive directed the Secretary of Homeland Security to create a national level Domestic Nuclear Detection Office within DHS. The Secretaries of State, Defense, and Energy as well as the Attorney General were ordered to assign personnel to staff this new organization and to lend expertise to strengthen the development and deployment of a detection system, coordinate the detection effort with the other government entities in the United States, and develop a global nuclear detection architecture consisting of domestic and international portions. The Departments of Defense, State, and Energy would design and implement the international segment.[39]

June 2005 marked a critical milestone in reshaping DoD's approach to its homeland defense and support to civil authorities' missions through the development and approval of DoD's *Strategy for Homeland Defense and Civil Support*. Although Secretary Rumsfeld directed the formulation of the strategy in the Strategic Planning Guidance of March 2004, internal delays and bureaucratic resistance associated with organizational change hampered progress. Nonetheless, these impediments were ultimately overcome, and the strategy represented the Department's vision for transforming homeland defense and civil support capabilities.

The strategy specifically concentrated on DoD's paramount goal: securing the United States from direct attack. Recognizing the sensitivity associated with the role of the military in domestic affairs, the strategy made clear that it was rooted in a respect for America's constitutional principles. The strategy also sought to capitalize on Secretary Rumsfeld's commitment to transformation of U.S. military capabilities. Thus, it examined a ten-year period and gave equal recognition of terrorist and state-based threats to the United States.[40]

The strategy's foundation was the concept of an active, layered defense outlined in the *National Defense Strategy*. Specifically, this active, layered defense is understood to be global, seamlessly integrating U.S. capabilities in the foreign regions of the world, the global commons of space and cyberspace, in the geographic approaches to U.S. territory, and within the United States. In short, it is defense in depth predicated on viewing the strategic environment as an open system in which people, trade, and information move continuously and for which the entire U.S.

Government contributes to its defense through a variety of capabilities in a synchronized manner. For an active, layered defense to be effective, it "requires superior intelligence collection, fusion, and analysis, calculated deterrence of enemies, a layered system of mutually supporting defensive measures that are neither ad hoc nor passive, and the capability to mass and focus sufficient warfighting assets to defeat any attack."[41]

Although the concept of an active, layered defense had a global context, the strategy focused primarily on the U.S. homeland and the approaches to U.S. territory. The Defense Department recognized its responsibility for a number of activities in these geographic layers, but as an organizing construct, there were three principal categories: "Lead, Support and Enable." "Lead" meant that DoD, at the direction of the President or the Secretary of Defense, executed military missions to dissuade, deter, or defeat attacks on the United States. "Support" considered DoD's traditional role of providing support to civil authorities at the direction of the President or Secretary of Defense. This support was to be part of a comprehensive national response to prevent or protect against terrorist incidents or to recover from an attack or disaster. Finally, "Enable" sought to enhance the homeland security and homeland defense capabilities of domestic and international partners and, in turn, improve DoD capabilities by sharing technology and expertise across military and civilian boundaries. The strategy also addressed key objectives of this three pronged framework as well as specific operational capabilities that were needed to achieve these objectives and the strategic risks of not doing so.[42] In addressing capabilities the authors of the strategy sought to influence other departmental processes, namely, funding, force structure, and technology development, in order to implement the strategic tenets of the document. The next opportunity to have an influence on these processes would be the QDR. However, before that review occurred, an incident of national significance[43] would also have an effect.

On August 29, 2005, the most destructive hurricane in U.S. history, Katrina, hammered the Gulf of Mexico, killing more than a thousand people and causing substantial devastation to the states of Louisiana, Mississippi, and Alabama. New Orleans bore the brunt of the damaging effects when the powerful storm breached the levee system and flooded eighty percent of the city.[44] Public order disintegrated because of inadequate planning by municipal and state officials and a lack of foresight regarding potential scenarios when a category 5 hurricane hits. The federal response proved unequal to the task as well, and poor communication and coordination between federal and state authorities only exacerbated the deficient response effort. FEMA was overwhelmed by the magnitude of the destruction and the requests for assistance. It soon became apparent that even with the support of other civilian agencies, DoD and National Guard units from across the country would need to be deployed.[45]

Ultimately, more than 72,000 active duty military and National Guard personnel deployed to provide assistance to ravaged areas between August 29 and September 10. The figure was twice the record deployment of military assets in response to a natural disaster since Hurricane Andrew in 1992. The department acted on more than 90 requests for assistance from civil authorities, many of which were approved orally by the Secretary of Defense, including one that had an estimated value of one billion dollars. There were deficiencies in the Department's response such as lack of pre-planned response capabilities for possible disaster scenarios, the need for closer coordination between DHS and Northern Command, and the requirement for more accurate and rapid initial damage reconnaissance and assessment. Nonetheless, the DoD evaluation was that U.S. military forces were ready and capable to execute the largest, most comprehensive, and most responsive civil support mission ever.[46]

Overall, the media, the American public and federal authorities rated DoD's response a success. When departmental advocates pointed out, however, that an even more robust DoD response might be required in the event of a catastrophic terrorist event where the loss of life and destruction of property would exceed Katrina's devastation, the argument was dismissed because of the department's successful response.[47] The DoD leadership overseeing the ongoing QDR, which examined U.S. defense strategy in late 2005 and resulted in a report to Congress in February 2006, paid scant attention to homeland defense and civil support issues. In short, the touting of DoD's rapid and dependable response before congressional committees and in the media made these issues victims of their own success.

Publication of the QDR report is certainly not the end of DoD's involvement in homeland defense or support to civil authorities. While publication of the DoD *Strategy for Homeland Defense and Civil Support* represents the zenith of attention to these missions, the QDR review represented a plateau. The QDR report itself signaled that the Department's leadership felt confident that in the more than four years since the tragic events of September 11, 2001, DoD had made substantial progress in improving its capability to protect the U.S. homeland from attack and to respond effectively to a catastrophic event. The latter was a capability that required further attention, as the QDR report noted, but it was not the priority. Iraq and Afghanistan were consuming the leaders' attention and the Department's resources. As the QDR report noted, DoD believed that the civilian agencies that had these missions as their primary responsibility needed to attend to them. It was a position with which the Secretary of Homeland Security and the Congress agreed. The former stated that an enhanced FEMA was needed, and the Congress obliged him by passing the FEMA Reorganization Act in 2006. For many, DoD had amply proved its ability to fulfill its three roles specified in its own strategy: lead, support and enable. For its part, the Department was confident in its strategy and its ability to accomplish the homeland defense mission.

END NOTES

1. Bruce Maxwell, *Homeland Security: A Documentary History*, Washington, DC: CQ Press, 2004, pp. 241-242.

2. Ibid., p. 242.

3. *9/11 Commission Report*, Final Report of the National Commission on Terrorist Attacks Upon the United States, New York: W. W. Norton & Co., 2004, p. 336.

4. Illustrative are: *New World Coming: American Security in the 21st Century*, United States Commission on National Security/21st Century Report, September 15, 1999; *Assessing the Threat*, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction Report, December 15, 1999; and *Countering the Changing Thereat of International Terrorism*, National Commission on Terrorism Report, 5 June 2000.

5. John Woolley and Gerhard Peters, The American Presidency Project [online]. Santa Barbara, CA: University of California, hosted, Gerhard Peters, database, available from *www.presidency.ucsb.edu/ws/?pid=438*.

6. Esther Schrader, "America Attacked; Policy Changes," *Los Angeles Times*, 16, Sept. 2001, p. A12.

7. Ibid.

8. Robert J. Bartley, "Thinking Things Over: Pentagon Fires and Pentagon Reform," *The Wall Street Journal*, 17, Sept. 2001, p. A23.

9. Vernon Loeb, "Pentagon Says Homeland Defense Is Top Priority," *The Washington Post*, 2, Oct. 2001, p. A23.

10. Department of Defense, *Quadrennial Defense Review Report*, Washington, DC: U.S. Department of Defense, 30, Sept. 2001, p. 19.

11. "Homeland Security In a Pentagon Post," *The New York Times*, 3, Oct. 2001, p. B7.

12. Thomas E. Ricks, "Military Overhaul Considered," *The Washington Post*, 11, Oct. 2001, p. A1.

13. Bill Miller and Eric Pianin, "National Guard's Airport Role to End," *The Washington Post*, 24, Jan. 2002, p. A8.

14. Edward Rowny, "Homeland Defense Needs a Real Commander," *The Wall Street Journal*, 14, Feb. 2002, p. A20.

15. Greg Jaffe, "Homeland Defense to Receive Higher Priority in New Command," *Wall Street Journal*, 17, Apr. 2002, p. A4.

16. Donald Rumsfeld, Testimony before the United States Senate Appropriations Committee, 7, May 2002.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. Thomas E. Ricks, "Bush Plans to Tap Ex-Lawmaker for New Defense Post," *The Washington Post*, 2, July 2002, p. A13.

22. Nicholas Kulish, "House Panel Votes Down Parts of Homeland-Security Plan," *Wall Street Journal*, 12, July 2002, p. A4.

23. Ibid.

24. William M. Arkin, "The Best Defense," *Los Angeles Times*, 14, July 2002, p. M1.

25. Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* 81, No. 3, May/June 2002, pp. 20-32.

26. Bradley Graham and Susan Schmidt, "Homeland Office Promises Investigation," *The Washington Post*, 2, Feb. 2003, p. A5.

27. George W. Bush, "Homeland Security Presidential Directive-5, Management of Domestic Incidents, 28, Feb. 2003.

28. "Rumsfeld's Second Front," *The Wall Street Journal*, 1, April 2003, p. A14.

29. Paul McHale, Testimony before the 108th Congress, United States Senate Armed Services Committee, 8, April 2003.

30. George W. Bush, "Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection," 17, Dec. 2003.

31. George W. Bush, Homeland Security Presidential Directive-8, National Preparedness, 17, Dec. 2003.

32. John Mintz, "U.S. Threat Level Rises to Orange; Attack Risk May Be Highest Since 9/11," *The Washington Post*, 22, Dec. 2003, p. A1.

33. Paul McHale, Hearing Statement, 108th Congress, U.S. Senate Armed Services Committee, 25, Mar. 2004.

34. Ibid.

35. George W. Bush, Executive Order 13354, National Counterterrorism Center, August 27, 2004. In December 2004, Congress codified the NCTC in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and placed the NCTC in the Office of the Director of National Intelligence.

36. U.S. Department of Homeland Security, *National Response Plan*, Dec. 2004.

37. George W. Bush, National Security Presidential Directive-44/Homeland Security Presidential Directive 13, Maritime Security Policy, 21, Dec. 2004.

38. Spencer S. Hsu and John Mintz, "Military Was Set To Down Cessna; Authority Granted As Plane Strayed Deep Into Capital," *The Washington Post*, 26, May 2005, p. A1.

39. George W. Bush, National Security Presidential Directive-45/Homeland Security Presidential Directive-14, Domestic Nuclear Detection, 15, Apr. 2005.

40. U.S. Department of Defense, *Strategy for Homeland Defense and Civil Support*, Washington, DC: US Department of Defense, 2005, p. 1.

41. Ibid., pp. 1-2.

42. Ibid., pp. 2-4.

43. U.S. Department of Homeland Security, *National Response Plan*, December 2004, p. 3. "Incidents of National Significance are those high-impact events that require a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, private-sector, and nongovernmental entities in order to save lives, minimize damage, and provide the basis for long-term community recovery and mitigation activities."

44. Gary Gilmore, "Assistant Secretary McHale: DoD Acted Quickly to Provide Post-Katrina Support," U.S. Department of Defense, American Forces Information Service Press Release, 13, Mar. 2006.

45. The White House, *The Federal Response to Hurricane Katrina: Lessons Learned,* Washington, DC: Executive Office of the President, February 2006, pp. 1-3, 51-64; U.S. Senate, *Hurricane Katrina: A Nation Still Unprepared,* Washington, DC: Committee on Homeland Security and Government Affairs, 2006, pp. 1-19; U.S. House of Representatives, *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, Washington, DC: U.S. Government Printing Office, 2006, pp. x-xi, 1-5.

46. Gilmore, "Assistant Secretary McHale: DoD Acted Quickly to Provide Post-Katrina Support," Statement by Paul McHale, Assistant Secretary of Defense for Homeland Defense, before the 109th Congress, Committee on Appropriations, Subcommittee on Defense, U.S. House of Representatives, 28, Sept. 2005.

47. Geoff Fein, "Katrina Showed Need for Rapid Damage Assessment," *C4I News,* 3, Aug. 2006, p. 1.

Note: This article was originally published in the June 2008 issue of *U.S. Army War College Guide to National Security Issues,* Volume II, *National Security Policy and Strategy*.

New Requirements for a New Challenge: The Military's Role in Border Security

Bert Tussing

Reprinted with permission from *Homeland Security Affairs.*

Introduction

Threats along America's borders have taken on a new and ominous character. In the past, United States customs and border officials were focused on relatively benign matters of enforcing laws surrounding trade and immigration, protecting agriculture and economic interests from pest and disease, and processing people, vehicles and cargo.[1] In the last three decades, however, these issues have been joined, and eclipsed, by growing apprehension surrounding matters of far greater concern than illegal immigrants in search of economic opportunities. The migration of gangs across the nation's borders and into our cities, organized criminal elements trafficking drugs and human beings into the United States, and the specter of terrorists and terrorist devices seeping through our borders to the north and south, all combine to contribute to a growing set of dangers to our people. Moreover, a compounded threat is emerging at the intersection of these concerns, wherein criminal and terrorist elements may unite toward the attainment of shared and separate goals. The combination of these elements elevates the potential disruption to our society beyond the responsibilities of law enforcement to matters of defense.

As the nature and severity of the threat increases, the character of our response to it must change. This country has a cherished tradition of separation between its police and its military. That tradition has generally delegated responsibility for keeping the citizenry safe from internal, domestic dangers to federal, state, and local law enforcement agencies. Likewise, safeguarding that citizenry from external aggression has, for the most part, been the obligation of the United States armed forces. But in a time where criminal and terrorist activities may merge at our borders, this distinction may not be maintainable. New cooperation is mandated between the military and the border patrol. In terms of that cooperation, the military must be prepared to assume a greater role.

An Over-taxed Border

No one seems to underestimate the urgency of the requirement. Nor have they since before 9/11. The United States Commission on National Security/21st Century, commonly known as the Hart-Rudman Commission, recommended that the executive branch establish a "National Homeland Security Agency." Among other things, this agency would encompass the Customs Service, the Border Patrol, and the United States Coast Guard in a synergistic environment to patrol U.S. borders and police the flow of peoples and goods through hundreds of ports of entry.[2] Legislation creating the Department of Homeland Security (DHS) included border and transportation security as one of the original five under-secretariats. When Secretary Michael Chertoff came to Washington in February 2005, he entered the department with "six priorities;" the third of those was to "strengthen border security and interior enforcement…"[3] The new secretary would make his concerns clear as he unveiled a new organizational structure that would remove bureaucratic layers between his office and customs and border protection as part of an effort to …gain full control of our borders to prevent illegal immigration and security breaches. Flagrant violation

of our borders undercuts respect for the rule of law and undermines our security. It also poses a particular burden to those in our border communities. We are developing a new approach to controlling the border, one that includes an integrated mix of additional staff, new technology and enhanced infrastructure investment.[4] Institutionally, the requirement for a robust border security mechanism seemed clear.

Functionally, the requirement was even clearer. In the best of times, under the best of circumstances, the need for diligence at the border is compelling. On a typical day, more than 1.1 million passengers and pedestrians, including 635,000 aliens, over 235,000 air passengers, over 333,000 privately owned vehicles, and over 79,000 shipments of goods are processed at the nation's borders.[5] Every year U.S. Customs and Border Protection (CBP) processes nearly half a billion people, 130 million trucks and cars, and 20 million cargo containers through 325 ports of entry.[6]

Curiously enough, however, the immensity of the daily requirement is not the most compelling factor among concerns over the security of the border. What is described above is the routine, legitimate traffic that allows for the free flow of visitors and commerce, keeping open the doors of the "land of opportunity" and, coincidentally, sustaining much of the economy. The greater concern for security lies beyond these factors in an accompanying flow that does not seek legitimate opportunity, but criminal gain; that is not interested in sharing the American way of life, but in undermining it and the institutions and values which sustain it. A report developed in the House of Representatives' Committee on Homeland Security offers an interesting and potentially ominous contrast: During 2005, Border Patrol apprehended approximately 1.2 million illegal aliens [along the Southwest border between the United States and Mexico]; of those, 165,000 were from countries other than Mexico. Of the non-Mexican aliens, approximately 650 were from special interest countries. [7, 8]

The threat along the northern border, while far less publicized, is nevertheless cause for concern; perhaps equal concern, perhaps greater. In 1988, U.S. Customs officials arrested three members of a Syrian terrorist group, linked to al Qaeda in the process of entering the U.S. with explosives.[9] Members of the terrorist cell that executed the 1993 attack on the World Trade Center entered the U.S. from Canada, and were planning to use Canada as a possible escape route. In December 1999, Ahmed Ressam was arrested crossing into the United States in possession of bomb making materials and plans for what became known as the Millennium bomb plot against Los Angeles International Airport.[10] Ressam would be characterized by the State Department as a textbook example of someone who "capitalized on liberal Canadian immigration and asylum policies to enjoy safe haven, raise funds, arrange logistical support, and plan terrorist attacks."[11]

And the past, we have every reason to fear, may well be prelude, as pointed out by Dr. Todd Hataley of the Royal Military College of Canada: In the post 9/11 period Canada has continued to raise security concerns in the United States. U.S. security officials believe that Canada is not only home to "sleeper cells" waiting for a chance to cross the border and attack the United States, but also that crossing from Canada has become a favorite route for illegal immigrants, drug smugglers, and potential terrorists.[12]

The Military in (limited) Support

Juxtapose this history against a northern border that stretches nearly 5,000 miles and a southwestern counterpart that runs another 2,000, and the challenge weighing against CBP is irksome, to say the least. In October 2006 there were 11,000 agents assigned to watch and protect

both sets of borders.[13] In May 2006, the Administration embarked upon a plan to raise those numbers to over 18,000 by the end of 2008,[14] increasing the total number to over 101% of the number that stood when the president took office in 2001.[15]

Whether or not that number will be sufficient is debatable. Whatever the case, plans for the *future* do not meet a requirement facing us *today*. The challenges that have inspired these increases will not be suspended until the increases can be brought about. As though acknowledging the same, the Administration launched Operation Jump Start in May 2006. The operation was officially terminated on July 15, 2008,[16] but at its height included over 6,000 National Guard from forty-eight states, brought to "strengthen border security and encourage deterrence."[17] David V. Aguilar, chief of the Office of Border Patrol for CBP, testified as to the nature of the Guard's mission before members of the House Homeland Security Committee:

National Guard units will assist DHS by executing missions such as logistical and administrative support, operating detection systems, providing mobile communications, augmenting DHS's border-related intelligence analysis efforts, building and installing border security infrastructure, providing transportation and training.[18] It is important to note, however, that while the presence of the Guard allowed CBP agents to return focus to law enforcement activities along the border, the troops did not join the agents in those activities, nor were they ever intended to do so. At the same hearing, Chief Aguilar was quick to remind the Congress of one clear distinction between the National Guard and the CBP mission. However, law enforcement along the border between the ports of entry will remain the responsibility of Border Patrol agents. The National Guard will play no direct law enforcement role in the apprehension, custodial care or security of those who are detained.[19]

This pronounced distinction in the roles that the National Guard may assume in border operations may seem confusing. After all, the immediate requirement that saw the deployment of Guard seems to invite additional manpower on the border to assist in surveillance, intervention, apprehension, and arrest. In the face of the immensity of their task, CBP lauding the fact that 6,000 National Guard allowed the Border Patrol to return 350 agents to "traditional frontline duties"[20] could easily lead to questions as to why more Guard could not be positioned on those "frontlines."

Those slightly schooled in laws and regulations surrounding the issue of military support to law enforcement agencies may still be confused. The hub of much of the discussion surrounding these issues is the Posse Comitatus Act, legislation enacted in the immediate aftermath of the Civil War, which largely prohibits the use of the active duty armed forces in executing the domestic laws of the United States.[21] Note, however, that the act only applies to *federal* forces. It does not apply to the National Guard, unless the Guard forces in question have been "federalized," or mobilized under Title 10 of the United States Code to perform a federal mission. Title 10, for instance, is the authority under which National Guard units are serving overseas in support of the United States' mission in Iraq. If the Guard forces are either in a "state active duty" status, or serving under the authority of Title 32 of the United States Code (a status that has the forces sustained by funds from the Department of Defense but retained under the command and control of the state governors and their adjutant generals), National Guard forces may serve in a direct law enforcement function.[22] Why, then, the distinction, and restriction, in border operations in the Southwest or any other operations of this sort? Perhaps even more to the point: Why restrict the military–active or reserve–from directly supporting the law enforcement function of the border security mission?

Soldiers–Not Policemen

The motivation behind the restriction is, perhaps, uniquely American and embedded in our national mindset. Simply stated, the people of the United States do not want our soldiers to be policemen, or our policemen to be soldiers. The philosophical underpinnings of this aversion can be traced to the colonies of the pre-Revolutionary War, when the heretofore loyal subjects of Great Britain were repulsed by oppressive measures like the Quartering Acts that cast the British forces in the role of overseers and, even, oppressors.[23] These same attitudes emerged at the end of the Reconstruction following the Civil War, when the federal military stood as an occupying force over the former Confederate states. These historic examples – combined, perhaps, with persistent images of military oppression that accompanied much of our immigrant ancestry from overseas – may help us to understand our citizenry's aversion to too much of a military presence for too long in our streets. Consider, for instance, what may be thought of as the subliminal response to the presence of the military in our nation's airports following 9/11. Initially the sight of soldiers along the concourses of O'Hare and Kennedy International kindled an air of assurance and accompanying goodwill. But how long was it before some of us were asking "Why are these military people here, with those rifles and that equipment?" The truth is Americans live in a state of dichotomy regarding attitudes about the military. We appreciate their sacrifice. We acknowledge their dedication. We take pride in their prowess and the virtue of their leadership. But we are dedicated to the proposition that these soldiers will ever remain the servants of the people, and not our overseers.

Fortunately, few are more sensitive to the military's role than the military's leadership. The clear distinction between the roles and responsibilities of law enforcement and the military is ingrained in the mindset of its generals. Any number of reasons could be cited for this sensitivity, beginning with the fact that the country's all-volunteer force is very much a military "of the people" and therefore very much "for the people." Moreover, the senior leadership currently directing our armed forces evolved from a generation of young officers born in the shadow of the Vietnam era.[24] The soldiers, sailors, airmen, and Marines of that era undeservedly bore the derisive brunt of a society turned sour on the war. In the same time period, reports of the Pentagon gathering intelligence against anti-war groups further broadened the divide between much of America and her military. Institutional assurances were put in place in the 1980s to prevent this type of surveillance from ever occurring again;[25] but having survived that era of distrust between the nation's people and the nation's military, the current uniformed leadership is keenly aware of how important the support of the citizenry is to its soldiers – and how fragile.

Nothing New in the Requirement?

Even so, Chief Aguilar reminds us that border security operations involving the National Guard are not a requirement unique to the new century: Let me first state that National Guard support and coordination with DHS and the Border Patrol is nothing new. While this new infusion will be on a larger scale, the Border patrol has a history of nearly two decades working with National Guard units to utilize their unique expertise, manpower, technology and assets in support of our mission and as a force multiplier.[26]

In fact, recent history witnessed the United States military's involvement in border security operations not only by the National Guard, but by the active duty component as well. In response to a growing connection between border security and counter-narcotics programs in the 1980s, President Ronald Reagan signed a National Security Decision Directive that simultaneously described drug trafficking as a threat to national security and authorized military involvement in combating it.[27] In 1989, the military's Joint Task Force 6 (JTF-6) was created to coordinate

its expanding support for "the anti-drug efforts of border region police agencies, including the Border Patrol."[28] Like the Guard, this task force would eventually play an important role in constructing physical barriers designed to slow or channel the flow of illegal immigrants. Unlike the Guard, JTF-6 also deployed aviation assets and ground troops along the border.[29]

Support for the military's role along the border continued through the 1990s. In 1991, key legislation was passed that codified a consensus to allow the Department of Defense to support any agency of the federal government with counterdrug responsibilities. More noteworthy yet, the legislation opened the way for DoD support to state and local government law enforcement agencies in achieving the same ends.[30] In 1997, the United States House of Representatives passed a resolution calling for the deployment of 10,000 additional troops in support of counterdrug operations along the southwest border.[31]

Tragedy was to interrupt the final passage of that resolution. On the evening of May 20, 1997, eighteen-year-old Ezequiel Hernandez was herding goats when he was mistakenly shot by the leader of a Marine rifle team that was observing an area of the Rio Grande known for its illegal drug trafficking. The Marines were members of JTF-6 and had been acting in support of the Border Patrol, but had received no civilian law enforcement training or briefings on local conditions.[32]

The outcry against the tragic occurrence would eventually subside across most of the social landscape, but not from the perspective of the military. Returning to its traditional degree of reticence, the Pentagon's leadership withdrew its armed forces from the border and levied new restrictions that would cast the military in a predominantly technical-support capacity. In the future, JTF-6 would be re-designated Joint Task Force-North and the personnel-intensive, boots-on-the-ground support provided by the unit in the 1990s would be replaced along the border with ground sensors, radar, airborne platforms, and thermal imagery. Deliberately postured in support of federal, state, and local law enforcement entities, the command's website notes that its technological focus has allowed for a reduction in manpower requirements.[33] But the first, and perhaps most significant, reduction came in terms of troops on the ground.

This would largely characterize the military's consistent role, for both the active and reserve components (including the National Guard) from the time of the tragedy in Texas until the calamity of September 11, 2001. In the aftermath of the attacks on the World Trade Center and the Pentagon, immediate steps were taken to reinforce the security of the nation's borders. Along entries from both north and south, the president commanded the deployment of roughly 1,600 National Guard troops for six months to support federal border officials.[34] New emphasis in maritime and aviation security along, within, and through the approaches to our borders became accompanying measures to land border security, and were formalized in interagency strategies.[35]

In the midst of these events, the United States Northern Command (NORTHCOM) was established on October 1, 2002 "to provide command and control of Department of Defense (DoD) homeland defense efforts and to coordinate defense support of civil authorities."[36] The new combatant command, primarily responsible for active service components' activities within the domestic confines of the United States, was charged in their mission statement to: Deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within its assigned area of responsibility; and as directed by the President or the Secretary of Defense, provide military assistance to civil authorities, including immediate crisis and subsequent consequence management operations.[37]

This mission statement instantly distinguished the new command from its counterparts overseas. The first part of the mission was reasonably clear, if ominous. "Deter, prevent and defeat" could be realistically expected as part and parcel of a military mission anywhere around the globe. The armed forces of the United States identify with this language and are fully prepared to do whatever is required to fulfill this mission. But the second half of the command's mission statement (euphemistically referred to across the military as the "right of the semicolon" requirement) was less intuitive, and arguably more complex than the first. The powerful segue – "as directed by the President or the Secretary of Defense" – is indicative of a very measured approach to this part of the mission. Placing the military in support of civil authorities will concurrently place them in activities normally conducted and controlled by those authorities. And the closer the military comes to controlling civil activities, the less comfortable it finds the mission.

A Shift in Focus: Counterdrug to Counterterror

The military's directives support its reticence. Civil support is characterized by the Department of Defense as granted in response to domestic emergencies and "for designated law enforcement and other activities."[38] However, the DoD directive regulating military support to civilian law enforcement agencies specifically prohibits the use of the military for interdiction; search and seizure; arrest, apprehension, stop and frisk or similar activity; and the use of military personnel in the pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.[39]

As the new structure of NORTHCOM was designed to meet the threat, along with a new office in the Department of Defense to oversee it,[40] the support mission for the military along the border was also changing. JTF-6, as previously noted, was redesignated JTF-North. This change in designation would mirror a change in focus, away from counterdrug operations to counterterror operations. Persistent, legitimate concerns over drug trafficking were being overshadowed by revelations of looming threats to our north and south. In Canada, as early as 1998, the Special Senate Committee on Security and Intelligence labeled the country as …a 'venue of opportunity' for terrorist groups: a place where they may raise funds, purchase arms, and conduct other activities to support their organizations and their terrorist activities elsewhere. Most of the international terrorist organizations have a presence in Canada. Our geographic location also makes Canada a favorite conduit for terrorists wishing to enter the United States, which remains the principal target for terrorist attacks worldwide.[41]

More recently, the same committee reported that "[a] relatively large number of terrorist groups [is] known to be operating in Canada, engaged in fundraising, procuring materials, spreading propaganda, recruiting followers and conducting other activities."[42]

To the south, there is growing concern over the opportunities being taken to transplant elements of international terrorist organizations among our closest neighbors. As early as May 2001, Adolfo Aguilar Zinser, former Mexican national security adviser and ambassador to the United Nations warned that "Spanish and Islamic terrorist groups are using Mexico as a refuge."[43] General James T. Hill, former commander of U.S. Southern Command, warned that the U.S. faces a growing risk, both from terrorist groups relocating to Latin America and "homegrown" groups originating therein. He warned specifically that Hezbollah and groups like it had established bases in Latin America, taking advantage of nearly ungovernable areas like the tri-border region between Brazil, Argentina, and Paraguay.[44] Add to these viable concerns over Venezuela's support to radical Islamic groups,[45] and the security concerns surrounding the well-being of our people at home continue to grow.

Unfortunately, as the military and the law enforcement agencies it supports along the border have moved on to this new concern, they can ill-afford to leave the old concerns behind. As though adding to the population of a snake pit, the arrival of terrorist concerns has done nothing to thin out the presence of drug traffickers among the cartels. Neither has it had an effect in reducing other organized-crime activities, like human trafficking, or diminishing a rise in criminal gang activity immigrating through Mexico into the United States. A majority report from the House of Representatives Committee on Homeland Security gave voice to these concerns, warning against "the triple threat of drug smuggling, illegal and unknown crossers, and rising violence" facing communities in the southwest.[46]

Criminals involved in this activity have taken on an air of arrogance that should further spur the nation's concerns. The aforementioned House study validates frequent reports that the cartels may be literally "outgunning" local law enforcement agencies on both sides of the border, possessing military-grade weapons, technologies and intelligence, and their own "paramilitary enforcers.[47]" The enforcers usually restrict their activities to actions against rival factions, but not always. In 2005, just hours after being sworn in as Nuevo Laredo's police chief, Alejandro Dominguez was killed. Dominguez came to office on the promise of cracking down on the cartels.[48]

This threat across the border should be enough to warrant alarm, but there are growing concerns that it cannot be contained there. Violence against U.S. law enforcement officials, from the Border Patrol to local law enforcement agencies, is rising at an alarming rate. From 2004 to 2005, attacks against Border Patrol agents on the Southwest border increased 108 percent. During fiscal year 2006 there were 746 violent incidents launched against these agents, including rock assaults, physical assaults, vehicle assaults, and firearm assaults. In March 2006, the House Judicial Committee's Subcommittee on Immigration, Border Security, and Claims conducted a hearing addressing these issues, noting a growing concern over law enforcement agents literally being "outmanned and outgunned" by criminal elements.[49] In January 2008, a U.S. Border Patrol agent was run down and killed near the Imperial Sand Dunes in Southern California, by men suspected of drug and alien smuggling.[50] And in what is perhaps the most blatant disregard for our territorial integrity so far, various cartel elements have recently initiated open attacks across our borders – against rival cartel members, against former Mexican law enforcement officials who have fled to the United States, and even against state and federal law enforcement officials.[51]

General Barry R. McCaffrey, former director of the White House Office of National Drug Control Policy, commented on the disturbing partnership growing between crime and terrorism at the nation's door. These groups are drawn together because of their complementary capabilities. Terrorists can create chaotic circumstances that allow for illicit activities. Criminal organizations have pre-established networks to move and sell narcotics and launder money.[52]

To date, the manifestations of this partnership have not taken on a character that would call for a military response. However, a recent report from Arizona indicates that a future requirement for the same is not beyond reason. Officials at Fort Huachuca, the nation's largest intelligence training center, changed security measures in May of last year after being warned that Islamist terrorists, with the paid assistance of Mexican drug cartels arranging their entry, were planning an attack against the post.[53] The plotters, up to sixty in number, were reported to be Afghan and Iraqi terrorists with high-powered weapons (including anti-tank missiles, Soviet-era surface-to-air missiles, and grenade launchers) smuggled into the United States through tunnels. The FBI would not elaborate on investigations surrounding the threat; neither would they comment on

other reports suggesting the "plot" was a Gulf cartel "plant" to bring in the U.S. military against a rival cartel. But an FBI representative did acknowledge that the report "demonstrates the cross-pollination that frequently exists between criminal and terrorist groups."[54]

The immediacy of genuine defense concerns, as opposed to law enforcement concerns along the border, is certainly open to question. Nevertheless, the evolving, intersecting threats of organized crime and terrorism, masked by the relentless challenge of illegal immigration across our borders, clearly present a dangerous and perplexing set of difficulties for federal, state, and local government officials. Law enforcement agencies across all three levels of government have the lead in addressing the difficulties. The military has been, and continues to be, in support. But is the current role being played by the military – under the current circumstances, against the current threat – appropriate?

Temporary, but Recurring?

As though hedging bets, all discussion of placing the military in support of border security operations in the United States is consistently couched in terms of temporary requirements. Such was the case in 2002; such was the case again in 2006. It is clear that the current Administration is making an honest effort in re-tooling Customs and Border Protection, in terms of both technology and "boots-on-the-ground" to meet the broader threat that has emerged since 9/11. The functions that have characterized DoD support along the border – communications and logistical support, lending and operating detection and sensor systems, augmenting border-related intelligence analysis efforts, training, and so forth – are being reflected in the strategic plans of the Department of Homeland Security in general and its Customs and Border Protection agency in particular. CBP's strategic plan specifically lays out a strategic objective to "maximize border security…through an appropriate balance of personnel, equipment, technology, communications capability and tactical infrastructure."[55] Moreover, the DHS is clearly intent on putting resources behind their rhetoric, as demonstrated by the fact that approximately half of its $5.4 billion information technology budget for 2008 will go towards developing and modernizing these capabilities.[56] Ostensibly, the intent is to enable CBP to completely take control of that part of the mission the military has served to supplement to date.

The question is, can we reasonably expect them to do that? Is it reasonable, for instance, to expect the Department of Homeland Security to duplicate the sensor capabilities that have been introduced in their support during this "period of transition?" Is it feasible and/or advisable for them to reproduce the communication suites that have supported their operations along the southwest border since 2006? Is it fiscally responsible to match the engineer assets that the military has introduced in support of the mission over the last few decades…and the maintenance capability…and the training capacity? To be sure, DHS has the means and the aptitude to address all of these functions to a degree; but does it have enough to meet the requirement posed by the threat according to our current assessment? And if it does, or shall soon, is it fair to assume that DHS will be able to meet the full evolving requirement to meet an evolving threat? Is it safe to make that assumption?

Planning for the Longer Term Against a Variable Threat

I would contend that it is not. The Department of Homeland Security's current direction towards strengthening border security will not, and can never, be the final solution. Trying to empower a single federal agency with the ability to solve foreseeable challenges in this area is neither feasible, nor advisable. Expecting our military forces to continue to "stand in the gap" in their present capacity is also ill-advised, whether referring to the federal component – our active duty

forces – or the "states militia" whose strength resides principally in the National Guard. A closer approximation of a solution to the evolving dilemma will begin with the realization that the border challenge must be addressed as a problem that varies with the introduction of a variable threat (See Figure 1).

Experience has taught us that the lower end of that threat is embodied in massive numbers of illegal aliens, albeit ones without malicious intent (indeed, a significant amount of the nation's concern in this regard is for the well-being of the aliens themselves).[57] It is reasonable to assign day-to-day cognizance over that end of the threat to Customs and Border Protection, as the clear "lead federal agency."

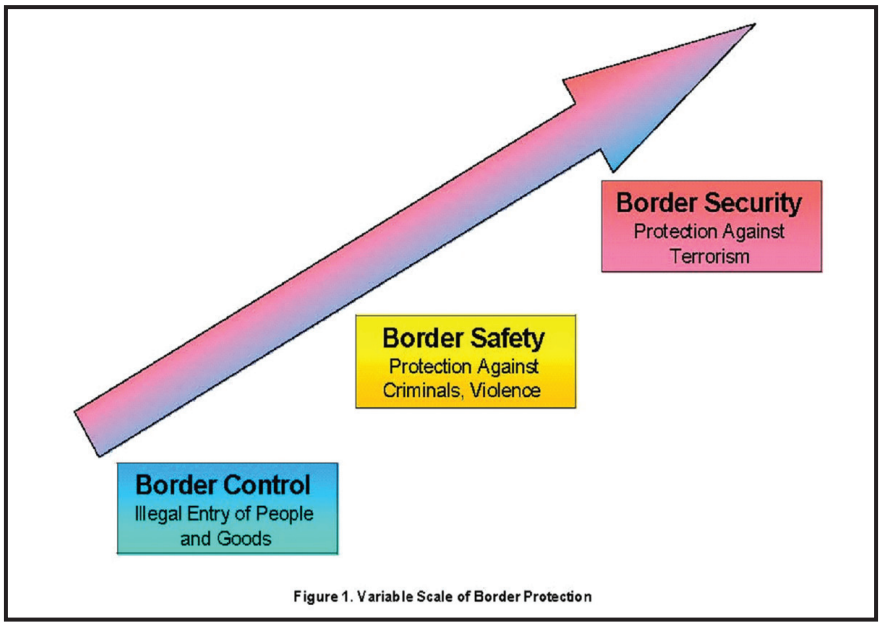


Figure 1. Variable Scale of Border Protection

As the threat moves further up the scale, however, we are introduced to an organized criminal element which has been seen trafficking both drugs and human beings. At this point, one might envision a requirement quite literally calling for greater force. That force could *begin* with a concentration and coordination of other law enforcement agencies (federal, state, and local). These would be keyed to their requirement by integrated information and intelligence from across the federal interagency. But they should also be served by mechanisms designed for intergovernmental intelligence and information exchange – up and down the chain between federal, state, and local authorities.

That exchange could also provide warnings and signals at the upper end of our threat spectrum, manifested in the aforementioned confluence of organized crime and international terrorism. In her study "U.S. Border Enforcement: From Horseback to High-Tech," Deborah Waller Meyers suggests that the difference in responding to the variations of the threat at our borders may parallel the difference between border control (protection against the illegal entry of people and goods), border safety (protection against criminals, violence, smuggling, etc.), and border security (protection against terrorists).[58]

Responsibility for security at the border, therefore, becomes a shared concern. Federal, state, and local government must arrive at a common understanding of what is needed to provide an acceptable level of security at the borders, and then determine a package to provide that security

that is feasible, affordable, and acceptable to the American people. Addressing our variable scale, therefore, begins in the federal government with an interagency plan, led by the Department of Homeland Security. The impetus for border protection that began with consolidating the nation's frontline border enforcement agencies under Customs and Border Protection must be continued to harness the support of other agencies (including but not limited to DoD) that have vital roles in meeting the complexities of the task. This will certainly include agencies like the Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency (DEA) whose traditional roles along both borders provide a background in both information and intelligence exchange and law enforcement. Multiple sectors of the intelligence community, led by DHS' own under secretariat for intelligence and analysis, can provide for the underpinnings of what the Department of Defense calls an "active, layered defense."[59] In turn, they will provide for the security of our borders, ideally well before the threat reaches it.

A stand-alone federal solution, however, will be one doomed to failure. Governor Janet Napolitano of Arizona begrudgingly acknowledged as much when she declared: "States are not responsible for operational control of international borders; however, due to the dire situation that exists along the United States-Mexico border in Arizona, the state has had to act to preserve the rights and bests interests of its citizens".[60]

Concerns mirroring those of Governor Napolitano, in Texas, New Mexico, and California, led to the memorandum of understanding signed between those states and the Department of Defense that served as the foundation for Operation Jump Start. Comparable shared concerns between the states of New York, New Hampshire, Vermont, and the federal government led to similar agreements in the initiation and execution of Operation Winter Freeze in 2004.[61]

Beyond these operations, a host of evolving mechanisms are being built to strengthen cooperative efforts between the three levels of government that could be trained to address concerns for border security. The FBI's Joint Terrorism Task Force offices located across the country (notably including cells in Phoenix, San Diego, and El Paso) could certainly be utilized towards these ends, bringing together representatives not only from state and local law enforcement, but agencies like the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Central Intelligence Agency, the Bureau of Immigration and Customs Enforcement, the U.S. Coast Guard, and DoD. Likewise, state fusion centers, financially sponsored in their development through grants from the Department of Homeland Security, are already serving as principal conduits for information exchange.

The military's role in the solution set that will be required in this combined interagency and intergovernmental solution, while occasionally cumbersome for the services, is inescapable. The expected transition described by the Bush Administration as the impetus behind Operation Jump Start may begin to solve the immediate problem at the lower end of the variable scale, but it should not be relied upon to address the middle and upper dimensions of its concerns. Even assuming CBP receives a significant infusion of resources to provide for technological solutions, that infusion will not take place overnight. While Operation Jump Start was officially terminated, counterdrug operation support is still being provided by our armed forces, Innovative Readiness Training (IRT) from the National Guard remains on the borders,[62] and sensor support operations from elements of both the active and reserve component remain underway.[63] The equipment and expertise currently being provided by the military will, for at least the time being, remain a requirement.

Moreover, technology can only serve to complement boots-on-the-border; it cannot replace them. Whether focused on interdicting the threat or – more ideally – deterring or preventing illegal transit, it is the physical presence of people that will actually accomplish the desired function. Again, DHS recognizes this reality and, along with the infusion of funds provided for technology along the border, is asking for an increase of $442.4 million to hire, train, and equip 2,200 new Border Patrol agents.[64] But these planned increases will not translate into immediate reinforcement along the borders. And, when spread across more than 7,000 miles of border to our north and south, 2,200 new agents may still project a degree of protection that is exceedingly thin. Therefore – even if only addressing the steady-state, lower-end requirement suggested by our variable scale – sufficient numbers for accomplishing this mission may only be available if the military remains actively engaged.

Keeping the military engaged and, as necessary, bolstering that engagement, will present a series of questions. First, the nation's leadership must decide which component of the military is best suited to address the issue along our variable scale: the active duty forces, or the National Guard, or both? Next, it will have to address the relative capacity of those forces to take on these responsibilities. Finally, having addressed the feasibility of the requirement, the leadership will have to return to the question of whether such engagement is advisable and, most importantly, acceptable in the eyes of the American people.

Active Duty Forces

Recent tradition shows that if an active component organization is involved in domestic civil support operations, its role is specialized and its numbers are small. A good example is the United States Marine Corps Chemical-Biological Incident Response Force (CBIRF). The CBIRF's mission requires it to respond to credible threats of a chemical, biological, radiological, nuclear, or high explosive yield incident in order to assist local, state, or federal agencies.[65] The unit lists an impressive array of capabilities to include agent detection and identification, casualty search and rescue, personnel decontamination, medical care, and stabilization of contaminated personnel.[66] However, the unit is composed of only 350 personnel and its mission is focused, and contained, around CBRNE (Chemical, Biological, Radiological, Nuclear, or High Explosive Yield) incident response. The United States Northern Command's Joint Task Force for Civil Support (JTF-CS) was also designed as a very specialized force, dedicated to planning and integrating consequence management support from the Department of Defense to civil authorities following a CBRNE incident. However, the task force is essentially a command and control entity, without assigned forces or dedicated transportation. In the event of a CBRNE crisis, several thousand personnel could be attached to JTF-CS by order of the secretary of defense to handle manpower intensive requirements alongside the specialized requirements the unit is uniquely qualified to fulfill.[67]

Joint Task Force North, as already noted, is much more directed to matters associated with the concerns of this article. The mission statement of the organization reiterates its relevance here.

"As directed, Joint Task Force North employs military capabilities to support law enforcement agencies and supports interagency synchronization within the United States Northern Command area of responsibility in order to deter and prevent transnational threats to the homeland".[68]

As is the case with much of the current National Guard mission along the southwest border, JTF-N has frequently assisted law enforcement efforts by means of detection and monitoring missions and by facilitating engineer support. This facilitation is brought about by the unit processing and prioritizing requests, and then sourcing those requests through appropriate active duty units.[69] In addition to these roles, however, the task force has played an important part in providing intelligence analysis and information sharing with federal, state, and local law enforcement agencies; other federal interagency partners; military units in support (from the active component, the service's reserves, and the National Guard); and (when authorized and appropriate) Canadian, Mexican, and other international partners by way of bi-national agreements.[70] Beyond this support, the task force has a history of conducting collaborative planning with federal, state, and local law enforcement agencies. This ability to plan for complex operations, incorporating bi-national, federal, state, and local stakeholders, highlights a core competency of the military and continues to prove more than beneficial in civil support missions inside and out of the United States.

Placed reasonably along the variable scale, the role of JTF-N could be seen in support of the Border Patrol in interdicting and arresting criminal elements, and intercepting and/or deterring the flow of terrorists over the nation's borders. While very deliberately not involved in arrest and apprehension themselves, the task force can support CBP as the primary law enforcement agency charged with that responsibility. Truthfully, if statutes and regulations were amended to allow JTF-N to join in those more direct functions, they are hardly configured to do so. Possessing approximately 150 soldiers, the unit's main contribution is in intelligence and information sharing, and in facilitating the introduction of other military forces to accomplish specified ends.

Perhaps curiously, JTF-N may be the only standing force from the military's active component dedicated to an aspect of land border security. Its ties to the mission are indirect, born out of a concern over the illicit flow of drugs across our borders; but the evolution of those counterdrug concerns to the newer concerns over counterterrorism will no doubt assure the task force's continued association with the CBP and its partner agencies.

In the meantime, there are other units whose missions could be applied to these endeavors, especially as concerns progress from border control, to border safety, to border security. The United States Northern Command itself may serve a vital liaison function between the militaries of the United States, Canada, and Mexico, ensuring transparency and encouraging cooperation through bilateral and multilateral Theater Security Cooperation Plans (TSCPs). NORTHCOM's Standing Joint Force Headquarters-North (SJFHQ-N) is poised as a deployable command and control element about which a Joint Task Force could be quickly configured in response to any number of homeland defense scenarios[71] – to include scenarios along our borders. Pre-designated Quick Response Forces in both the United States Army and the United States Marine Corps could rapidly fall in as the key components of those JTFs, if deployed. But they are not, nor are they envisioned to be, dedicated forces for those missions.

The National Guard

Then again, neither is the National Guard. Operation Jump Start, like the 2002 mission conducted in the wake of 9/11, was framed by the Administration as being an anomaly. Unless an unexpected turn of events lifts the threat from our borders, however, or a remarkable (some would suggest inadvisable) infusion of manpower takes place in the Border Patrol, it is likely to be a recurring anomaly. In spite of understandable reticence surrounding their use, no force recommends itself better to the mission than the Guard.

The thing that recommends the Guard most as the military resource of choice in support to civil authorities is its traditional relationship with those authorities. Recruiting offices across the country remind us of this relationship, an affinity born of both empathy and the proximity of the Guard to the people they serve. No one in the military is more attuned to the border enforcement, safety, and security challenges facing Yuma County, Arizona than the Arizona National Guard; no one in the armed forces is more aware of persistent concerns surrounding aliens of interest passing through the Swanton sector of New Hampshire, Vermont, and New York than their Guard. Likewise, no element of the United States military enjoys a closer working relationship with state and local government than those who dwell among them, exercise with them, and plan to respond to emergencies alongside them – in the National Guard.

Accordingly, logic continues to dictate that if greater forces are needed along the border, the Guard is the "go to" solution. The same thought process that calls for closer integration between federal, state, and local law enforcement extends easily to incorporating the local "state militia" in support of those integrated efforts. By further extension, as regional state cooperative efforts like the ones discussed here continue, cooperative, collaborative planning between the adjoining states' National Guard will provide a synergy that could "close the seams" between states' borders while simultaneously addressing the larger national border issue.

While the greatest urgency surrounding border security may exist in the states that constitute those borders, the cost for providing that security should not be theirs to bear alone. In fact, there are a number of precedents that have been set since 9/11 which allow for greater federal support to the states' immediate concerns. Notable among these are measures designed to fund deployment and employment of the National Guard in missions which remain under state control. For instance, Title 32 of the United States Code has been invoked by the secretary of defense in providing funds for state missions that remain under the authority of that state's governor as "necessary and appropriate" in supporting "homeland defense" activities.[72] Similarly, the potential exists for states' governors to fund National Guard activities undertaken in state active duty status through Department of Homeland Security grant monies.[73] Additionally, federal funding available to the states via 32 U.S.C. §112 for "drug interdiction and counterdrug activities" could logically be extended to a state force whose mission is tied to the federal effort to interdict these illicit activities coincident with the general policing of the nation's borders.[74]

Funding issues, however, become secondary when viewed against the greater concern of how the National Guard could afford the additional manpower demands implied in a recurring border security mission. A partial solution to this more immediate challenge to border states is to continue to augment their efforts with National Guard units from other states. Doing so would continue the pattern begun in 2002, revisited in Operation Winter Freeze, and most recently exhibited in Operation Jump Start. Officials are quick to point out that military readiness was not degraded by the Guard's participation in these endeavors.[75] Rather, the Guard's support has been portrayed as enhancing the engaged units' readiness in engineering, logistics, transportation, aviation, medical, and maintenance. Given continued federal funding, and accompanying cooperation among the states through the EMAC, this is a mechanism that could be applied to the problem for some time.

One should understand, however, that this is only a partial solution, and one that may not be sustainable. Indeed, rising demands, set against existing numbers in the Guard, may make sustainability the ultimate "deal breaker" in these discussions. The current strain being felt by the National Guard due to its employment at home and abroad is well documented. Expecting the

Guard to accept an increased burden by way of operations along the border amounts to what has been called "a further strain on already overextended military resources."[76] What most people fail to realize is that the National Guard has taken on these unprecedented demands, escalating from deployments in Bosnia-Herzegovina and Kosovo in the late 1990s and on through Operations Iraqi Freedom and Enduring Freedom, with historically weakened manpower rolls. Following the fall of the Soviet Union, the Guard was charged with making force reductions that have never been recovered. In 1989, the end strength of the National Guard stood at 570,000 personnel. Buoyed by the confidence of a "peace dividend" yet to be realized, that force has now been reduced by 20 percent to numbers that today stand at approximately 456,000, of which 350,000 are Army Guard.[77] Balance this depletion against the comparative operational tempo of the National Guard in the last three decades, and the picture becomes bleaker still. In the 1980s, serving Guard accounted for approximately 1 million man-days of duty per year. In the 1990s, (with a shrinking force), that figure had grown to 12.5 million man-days. In 2003, statistics showed that these figures had ballooned to 63 million man-days per year.[78]

It is beyond the intent of this article to suggest how many personnel are required to effectively secure the borders of the United States. In 2005, the late Representative Charlie Norwood (R-GA) sponsored a study that suggested 36,000 National Guard and/or authorized "State Defense Forces" would be required to assist the Border Patrol in securing the southwest border of the United States.[79] At one point before the activation of Operation Jump Start, the Administration had planned to deploy 1012,000 troops in support of the border patrol, as opposed to the 6,000 that were eventually sent.[80] Whatever the case, the numbers and the need that inspire them are more than appreciable. Combine concerns for the southwest border with the realization that our border with Canada is twice its size – and that there are only one-tenth the number of border patrol agents there as exist in the southwest to "protect" it – and the immensity of the requirement at hand becomes more appreciable still.

But up until this point we have only examined numbers, without coming to grips with how those numbers should be applied. It should be obvious that the 36,000-man augmentation envisioned in Congressman Norwood's study were not intended merely for surveillance, intelligence analysis, or engineering functions. They were intended to be postured as the deterrent effect that can only be supplied by boots-on-the-ground, standing in the gap, able to interdict and, as necessary, arrest and apprehend the threat to our people. They were intended to augment law enforcement agents alongside of those agents, occasionally providing peripheral support to their mission, but equally prepared to provide direct support to policing requirements. Were the threats we are facing still limited to those unintentionally accompanying the "huddled masses yearning to breathe free," the necessity for this augmentation would be significantly different. But that is not the case and the nation is obliged to prepare for a greater menace.

We are faced in the center and upper levels of our variable scale with a requirement that fails to fit comfortably in the realm of either law enforcement or national defense. Given the adversaries encountered in what has been called the "seam of ambiguity" between the two, the best path is to prepare to meet the trials of both environments. With all deference to the Department of Homeland Security and especially to their Border Patrol agents, it is illogical to expect them to be prepared for an upper-end threat that may see them outgunned. Neither is it logical to expect the American public to duplicate the assets and capabilities contained in the military to perform a function it should be capable of fulfilling. The reticence the armed forces have demonstrated in taking on the more direct involvement envisioned here is understandable – but perhaps misguided. Beyond the question of technology and manpower, of capabilities and numbers, the military requires a new mindset in addressing the border security issue.

The spirit embedded in the Posse Comitatus Act, and the laws and regulations which reflect it, is focused on reiterating and retaining the role of the military of the United States as the servant of its people. But the preponderance of the concern along our borders does not have to do with the comings and goings of the American people. Our concern is over the illegal entry into our country of those who wish to do us harm. The nation's primary defensive focus, as always, remains outward against an external threat – but that focus must now begin on the nation's shorelines and along its territorial boundaries. The studied hesitancy of leadership in the Department of Defense should be viewed against how quickly border enforcement issues could become border safety issues and, finally, reactive issues of national defense. An organization that justifiably prides itself on a preemptive mentality should bear no umbrage against employing itself as an obstacle to the threats envisioned here.

There is no doubt that these measures will require a reexamination of statutes, policies, and directives. But 9/11 has forced many such reexaminations. Moreover, the redirection envisioned here need not automatically alter the traditional relationship between America and its military concerning matters of domestic law enforcement. It will, however, automatically and exponentially emphasize a message of deterrence along our borders and bolster the means of defending those borders should deterrence fail.

Conclusion

Border security isn't what it used to be. Over the last three decades our concerns have steadily escalated from what was once as much a humanitarian issue as a security issue, to concerns over paramilitary violence, organized crime, and international terrorism. The requirements to meet these concerns have likewise increased, to the point that anything less than an interagency and intergovernmental response will inevitably leave the nation's citizenry vulnerable to a new and expanding series of threats.

One would like to think that the new era of threats to the country's borders and its people is a temporary condition and that the nation could soon settle back to a less demanding posture of readiness. Unfortunately, reality does not accommodate those wishes. The "long war" our leadership forecasts for the nation and our allies cannot be expected to remain "over there." Mr. Craig Duehring, principal deputy assistant secretary of defense for reserve affairs, framed the current state of affairs succinctly and with candor: "The nature of the mission has changed because of the Global War on Terrorism. The potential danger to our country has increased dramatically. It's not just a story of people looking for a better way of life. It is, in fact, a great potential for increased damage to our country, threats to our citizens, to our way of life. That's something that needs to be addressed. We took the border mission for granted for too many years, and that's no longer going to be the case".[81]

The new threat portends a new challenge for the military, both active and reserve components, from the United States Northern Command through to the individual states' National Guard. It will compel the military to revisit its thinking, motivation, and ethos in addressing this particular "law enforcement" requirement. The National Guard is by far the best tool to apply to the problem, but to do so must itself be re-tooled – principally in terms of numbers, but likewise in its predilection to take on a mission that normally resides outside of its traditional "lane." This should not imply, however, that the Guard should be the only military component focused on the problem. As the issue of security along the nation's borders climbs to concerns over protection against terrorism, assets and components of the active duty force, under the

direction of the NORTHCOM, must be folded into the process – first in terms of planning, and then, as necessary, in execution of those plans alongside their counterparts in the Guard. This coordination in planning and execution will be essential, as the National Guard will provide the foundation from which to launch a graduated response, if and when required.

Inevitably, a national strategy, emanating from the same impetus that launched Homeland Security Presidential Directives on maritime and aviation security[82] will be required for the land component of the nation's border protection. Reason and tradition dictate that the Department of Homeland Security takes the lead on the development of this strategy, with the Department of Defense heavily in support. When DoD's supporting role is portrayed, it should be as a reflection of an operational concept drawn up in cooperation and coordination between NORTHCOM and the National Guard Bureau. This strategy will require our government to decide from the depth and breadth of its capabilities which entities are best postured, best equipped, and best trained to meet the trials that lay ahead. Once those means are selected, however, they must come with an accompanying commitment from our government to ensure that they are sustainable. That sustainability must be measured in terms of equipment, in terms of technology and, above all, in terms of manpower.

Bert Tussing joined the Center for Strategic Leadership of the U.S. Army War College in October of 1999. His focus areas include homeland defense, terrorism, and Congress and military policy. In 2004, at the invitation of the assistant secretary of defense for Homeland Defense, he served on a senior advisory group to examine the development of a comprehensive strategy for DoD's role in homeland security. He is a senior fellow to George Washington University's Homeland Security Policy Institute; a senior fellow and adjunct faculty member of Long Island University's Homeland Security Management Institute; and on the Board of Experts of the University of California-Irvine's Center for Unconventional Security Affairs. In July 2005 he was appointed the Center for Strategic Leadership's director of homeland defense and security issues. Professor Tussing graduated with honors from The Citadel in 1975 and was commissioned a second lieutenant in the United States Marine Corps, where he served for twenty-four years. He holds master's degrees in national security and strategic studies (from the United States Naval War College) and strategic studies (from the United States Army War College). Mr. Tussing may be contacted at bert.tussing@us.army.mil.

End notes

1. U.S. Customs and Border Protection, Protecting America: U.S. Customs and Border Protection 20052010 Strategic Plan (Washington, DC: 2005), 3.

2. The United States Commission on National Security/21st Century, Phase III Report, *Roadmap for National Security: Imperative for Change,* February 15, 2001, 32-33, http://www.au.af.mil/au/awc/awcgate/nssg/phaseIIIfr.pdf.

3. Department of Homeland Security, "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," July 13, 2005, http://www.dhs.gov/xnews/releases/press_release_0703.shtm.

4. Department of Homeland Security, "Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks," July 13, 2005, http://www.dhs.gov/xnews/speeches/speech_0255.shtm.

5. U.S. Customs and Border Protection, Office of Field Operations, *Securing America's Borders at Ports of Entry: Strategic Plan FY 2007-2011* (Washington, DC: 2006), 2.

6. Ibid., "Message from the Commissioner."

7. United States House of Representatives Committee on Homeland Security, *A Line in the Sand: Confronting the Threat at the Southwest Border* (Washington, DC: 2006), 2.

8. "Special interest countries" are those designated by the intelligence community as countries that could export individuals seeking to bring harm to our country in the way of terrorism.

9. Christopher Sands, "Canada and the war on terrorism: The U.S. challenge on the North American front," *Canada Focus 2*, no.3 (October 2001), http://www.csis.org/component/option,com_csis_pubs/task,view/id,902/.

10. Deborah Waller Meyers, *U.S. Border Enforcement: From Horseback to High-Tech,* Migration Policy Institute Insight, no. 7 (November 2005).

11. Fred Burton, "U.S. Border Security: Looking North," *STRATFOR.com,* http://www.nixatron.com/StratT-bordernorth.htm.

12. T.S. Hataley, "Catastrophic Terrorism at the Border: The Case of the Canada-United States Border," *Homeland Security Affairs,* Supplement No. 1 (2007), 4, www.hsaj.org.

13. Committee on Homeland Security, *A Line in the Sand,* 2.

14. National Guard Bureau, Operation Jump Start Fact Sheet (Washington, DC:2006), http://www.ngb.army.mil/features/southwestborder/files/OJS_Fact_Sheet29Sept.doc.

15. House Armed Services Committee, National Guard and Border Security: Testimony of David V. Aguilar, Chief, Office of Border Patrol, U.S. Customs and Border Protection, Department of Homeland Security, 109th Cong., Sess. 2, May 24, 2006, 4.

16. Authors interview with Mr. David Lively, National Guard Bureau, August 29, 2008.

17. National Guard Bureau, Operation Jump Start Fact Sheet.

18. Testimony of David Aguilar, 3.

19. Ibid.

20. U.S. Customs and Border Protection Fact Sheet, *Operation Jump Start*, http://www.asisonline.org/newsroom/051506operationjumpstart.pdf.

21. The Act actually only prohibits the Army and, by extension, the Air Force that grew from it. It has been subsequently applied to the Navy and Marine Corps by policy and legislative supplement. There have been, nevertheless, both legislative and executive measures which have provided for rare exceptions in the military's direct support to law enforcement entities. For a complete discussion of the Act and its implications, see Charles Doyle, *The Posse Comitatus Act & Related Matters: the Use of Military to Execute Civilian Law,* Congressional Research Service Report 95-964.

22. For an expanded explanation of Titles 10, 32, and State Active Duty statuses of the National Guard, see Timothy J. Lowenberg, *The Role of the National Guard in National Defense and Homeland Security,* Vol. 2006 (Washington, DC: National Guard Association of the United States, 2005), 2-3, http://www.ngaus.org/ngaus/files/ccLibraryFiles/Filename/000000000457/primer%20fin.pdf.

23. The first Quartering Act (May 1765) provided that Great Britain could house its soldiers "in inns, livery stables, ale houses, victualling houses, and the houses of sellers of wine and houses of persons selling rum, brandy, strong water, cider or metheglin," and if numbers required in "uninhabited houses, outhouses, barns, or other buildings." It further required any inhabitants (or in their absence, public officials) to provide food and alcohol for the soldiers "without paying any thing for the same." A second Quartering Act (June 1774) was designed to restore imperial control over the American colonies. This became part of what the colonists would refer to as the Intolerable Acts. See David Ackerman's "The Tea Crisis and its Consequences through 1775," in Jack P. Greene and J.R. Pole, eds., The Blackwell Encyclopedia of the American Revolution (Malden, Massachusetts: Blackwell, 1999).

24. The current and immediate past Chairman of the Joint Chiefs of Staff served in Vietnam (or off the coast thereof). So, too, did the Vice Chairmen and the Chiefs of Naval Operations. The current Chief of Staff of the Army, Chief of Staff of the Air Force, and Commandant of the Marine Corps are not Vietnam veterans, but each of their predecessors was.

25. See, for instance, DoDD 5143.01, Under Secretary of Defense for Intelligence; DoDD 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight; and DoDD 5240.01, Department of Defense Intelligence Activities. The department's attitude is clearly displayed in the latter, leading its Policy section with the declaration: "All DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, Reference (c) [Executive Order 12333, United States Intelligence Activities, and Executive Order 13355, Strengthened Management of the Intelligence Community], the policies and procedures authorized herein, and other relevant DoD policies authorized by Reference (b) [DoDD 5143.01, Under Secretary of Defense for Intelligence]. *Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons."*(emphasis added)

26. Testimony of David Aguilar, 2.

27. Timothy J. Dunn, *The Militarization of the U.S.-Mexico Border 1978-1992: Low Intensity Conflict Doctrine Comes Home* (Austin, TX: Center for Mexican American Studies, University of Texas at Austin, 1996), 25.

28. Meyers, U.S. Border Enforcement: From Horseback to High-Tech, 4.

29. Dunn, The Militarization of the U.S.-Mexico Border 1978-1992, 153-154.

30. National Defense Authorization Act of 1991, Public Law 101-510, Section 1004.

31. For further information surrounding these recommendations, see the Report of Chairman Lamar Smith to the Subcommittee on Immigration and Claims of the Committee on the Judiciary of the House of Representatives, titled *Oversight Investigation of the Death of Esequiel Hernandez, Jr.,* 105th Cong., Sess. 2, November 1998.

32. Robert Suro, "Report: U.S. 'Failures' Led to Border Death," Washington Post, November 13, 1998. 33 Joint Task Force North, , http://www.jtfn.northcom.mil

33. Joint Task Force North, http://www.jtfn.northcom.mil.

34. Stephen R. Viña, Border Security and Military Support: Legal Authorizations and Restrictions, RS22443 (Washington, DC: Library of Congress, 2006), 5.

35. The White House, The National Strategy for Maritime Security (Washington, DC: 2005) http://www.whitehouse.gov/homeland/maritime-security.html; and The National Strategy for Aviation Security (Washington, DC: 2007) http://www.whitehouse.gov/homeland/aviation-security.html.

36. United States Northern Command website, http://www.northcom.mil.

37. Scott Shepherd and Steve Bowman, Homeland Security: Establishment and Implementation of the United States Northern Command, RS21322 (Washington, DC: Library of Congress, 2005), 1.

38. *Strategy for Homeland Defense and Civil Support* (Washington, DC: U.S. Department of Defense, June 2005), 5, http://www.fas.org/irp/agency/dod/homeland.pdf.

39. U.S. Department of Defense, *DoD Cooperation with Civilian Law Enforcement Officials,* DoD Directive 5525.5 (1989).

40. The Office of the Assistant Secretary of Defense for Homeland Defense, established under the authority of the Bob Stump National Defense Authorization Act of 2003, signed by the President on December 2, 2002.

41. Canada's Special Senate Committee on Security and Intelligence, *The Report of the Special Committee on Security and Intelligence* (Ottawa:1999).

42. Canadian Security Intelligence Service, *Public Report 2004-2005,* (Ottawa:2006), 2. http://www.csis-scrs.gc.ca/en//publications/annual_report/2004/report2004_e.pdf.

43. Ramón J. Miró and Glen E. Curtis, *Organized Crime and Terrorist Activity in Mexico, 1999-2002* (Washington, DC: Library of Congress, 2003), 43. http://www.loc.gov/rr/frd/pdffiles/OrgCrime_Mexico.pdf.

44. Chris Kraul and Sebastian Rotella, "Hezbollah presence in Venezuela feared," *Los Angeles Times,* August 28, 2008.

45. Ibid.

46. Committee on Homeland Security, *A Line in theSand,* 3.

47. Ibid., 4.

48. Ibid., 13.

49. House Judiciary Committee Joint Hearing before the subcommittee on Border Security, Immigration and Claims and the Subcommittee on Crime, Terrorism and Homeland Security, *Outgunned and Outmanned: Local Law Enforcement Confronts Violence Along the Southern Border,* 109th Cong., Sess. 2, March 2, 2006, www.hsdl.org/homesec/docs/legis/nps03-05240610.pdf&code=d2664b6364f601e7446d60362694349c.

50. Jerry Seper, "Mexico arrests suspect in U.S. agent's death," *Washington Times,* January 24, 2008.

51. "Mexico, U.S.: Threats of Cross-Border Cartel Killings," *Stratfor Today,* 26 August 2008. www.stratfor.com/analysis/mexico_u_s_threats_cross_border_cartel_killings_0.

52. GEN Barry R. McCaffrey and MAJ J.A.Basso, "Narcotics, Terrorism and International Crime: The Convergence Phenomenon," in R.D. Howard and R.L. Sawyer, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment* (Dubuque, IA: McGraw-Hill / Contemporary Learning Series: 2003), 323.

53. Sarah A. Carter, "Terrorist target Army base in Arizona," *Washington Times,* November 26, 2007. http://www.washingtontimes.com/article/20071126/NATION/111260034/1002.

54. Ibid.

55. U.S. Department of Homeland Security, Protecting America: U.S. Customs and Border Protection, 2005-2010 Strategic Plan (Washington, DC: 2005), 24.

56. Jill R. Aitoro, "Border security dominates DHS technology budget request," *Government Executive,* February 5, 2008, http://www.govexec.com/story_page_pf.cfm?articleid+39224.

57. Fact sheets on Operation Jump Start from Custom and Border Protection and the National Guard both list numbers of "Alien rescues" among their significant accomplishments.

58. Meyers, U.S. Border Enforcement: From Horseback to High-Tech, 22.

59. U.S. Department of Defense, Strategy for Homeland Defense and Civil Support.

60. Office of the Governor of Arizona, News Release, "Governor, Legislators, Visit Border Communities to see effects of Operation Strong Border, Secure Arizona," November 2, 2005, http://www.governor.state.az.us/press/2005/0511/NR~110205~Bordervisit.pdf.

61. Operation Winter Freeze was a designated National Special Security Event (NSSE) conducted by the Department of Defense in support of Border Patrol operations in its Swanton sector, encompassing 295 miles of continuous border between Canada and New York, New Hampshire, and Vermont. The sector had become notorious as the area with the largest number of Special Interest Aliens intercepted in the entire country. Conducted from 30 October 2004 to 26 January 2005, the operation was initiated in partial response to the terrorist attacks in Barcelona prior to their national elections and current intelligence data that highlighted the timeline between the presidential election of 2004 and Inauguration Day 2005 as a period of vital concern. Both active duty and reserve component assets were utilized in support of the event, but by far the greater percentage of support came from the National Guard. Ninety-three percent of the Task Force was Guard, hailing from twenty-one different states.

62. These IRT initiatives include Joint/multi-Service horizontal and vertical engineering projects in support of U.S. Border Patrol southwest border infrastructure objectives. Units and individuals are sourced through U.S. NORTHCOM's Joint Task Force -North. Training evolutions are scheduled and coordinated by National Guard-led IRT Task Forces. See Office of the Assistant Secretary of Defense for Reserve Affairs website, http://www.defenselink.mil/ra/html/irt.html.

63. Author's interview with Mr. Lively, August 29, 2008.

64. Katherine McIntire Peters, "Homeland Security seeks to bolster management, border security," Government Executive, February 4, 2008, http://www.govexec.com/story_page_pf.cfm?articleid=39217.

65. In addition, and unlike the National Guard's Weapons of Mass Destruction Civil Support Teams (WMDCST), CBIRF can also deploy overseas in support of the Unified Commands.

66. USMC Chemical Biological Incident Response Force, http://www.mnfwest.usmc.mil/public/iimefpublic.nsf/UnitSites/cbirf.

67. U.S. Northern Command, Joint Task Force Civil Support, http://www.jtfcs.northcom.mil.

68. U.S. Northern Command, Joint Task Force North, http://www.jtfn.northcom.mil/subpages/mission.html.

69. Lieutenant Colonel William J. Barnett, (Operations Officer, Joint Task Force North), telephone interview with the author, February 8, 2008.

70. Ibid.

71. U.S. Northern Command, "Standing Joint Force Headquarters North," http://www.northcom.mil/About/index.html.

72. 32 U.S.C.§905. Cited in Viña, Border Security and Military Support, 6.

73. Timothy J. Lowenberg, The Role of the National Guard in National Defense and Homeland Security,4

74. Viña, Border Security and Military Support, 5-6

75. House Armed Services Committee, Testimony of LTG H. Steven Blum, Chief, National Guard Bureau: National Guard and Border Security, 109th Cong., Sess. 2, May 24, 2006, 3

76. Peter Baker, "Bush Set to Sent Guards to Border," *Washington Post*, May 15, 2006.

77. Roger Allen Brown, *Sizing the National Guard in the Post-Cold War Era*, (Santa Monica, CA: Rand Institute, 1995), http://www.rand.org/pubs/research_briefs/RB7506/index1.html and Michael Waterhouse and JoAnne OBryant, *National Guard Personnel and Deployments: Fact Sheet*, RS22451 (Washington, DC: Library of Congress, 2007), 2.

78. Christine E. Wormuth, et al., *The Future of the National Guard and Reserves: the Beyond Goldwater-Nichols Phase III Report,* (Washington, DC: The Center for Strategic and International Studies, 2006), 32.

79. Frederick A. Peterson III and John E. Stone II, "Results and Implications of the Minuteman Project: A Field Report submitted to The Congressional Immigration Reform Caucus, (Washington, DC: Government Printing Office, 2005), 4.

80. John E. Stone, "*Operation Jump Start: Failure by Design,*" (Washington, DC:, U.S. Freedom Foundation, 2007), http://www,humanevents.com/article.php?print=yes&id=21993.

81. Craig Duehring, Principal Deputy Assistant Secretary of Defense for Reserve Affairs, quoted in Sgt Jim Greenhill's National Guard Bureau Press Release, "Operation Jump Start a success, officials say," December 11, 2006, http://www.ngb.army.mil/news/archives/2006/12/121106-OJS_success.aspx.

82. See HSPD-13, *Maritime Security Policy,* and HSPD-16, *Aviation Strategy,* both available at http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

Note: This article was originally published in the October 2008 edition of *Homeland Security Affairs.*

Border Security and Military Support: Legal Authorizations and Restrictions

Stephen R. Viña

Reprinted with permission from *CRS Report for Congress.*

Summary

The military generally provides support to law enforcement and immigration authorities along the southern border. Reported escalations in criminal activity and illegal immigration, however, have prompted some lawmakers to reevaluate the extent and type of military support that occurs in the border region. On May 15, 2006, President Bush announced that up to 6,000 National Guard troops would be sent to the border to support the Border Patrol. Addressing domestic laws and activities with the military, however, might run afoul of the Posse Comitatus Act, which prohibits use of the armed forces to perform the tasks of civilian law enforcement unless explicitly authorized. There are alternative legal authorities for deploying the National Guard, and the precise scope of permitted activities and funds may vary with the authority exercised. This report will be updated as warranted.

Background

The Secretary of the Department of Homeland Security (DHS) is charged with preventing the entry of terrorists, securing the borders, and carrying out immigration enforcement functions. The Department of Defense's (DOD) role in the execution of this responsibility is to provide support to DHS and other federal, state and local (and in some cases foreign) law enforcement agencies, when requested. Since the 1980s, the DOD (and National Guard), as authorized by Congress, has conducted a wide variety of counterdrug support missions along the borders of the United States. After the attacks of September 11, 2001, military support was expanded to include counterterrorism activities. Although the DOD does not have the "assigned responsibility to stop terrorists from coming across our borders,"[1] its support role in counterdrug and counterterrorism efforts appears to have increased the Department's profile in border security.

Some states, particularly those along the southern border that are experiencing reported escalations in crime and illegal immigration, are welcoming the increased military role and have taken steps to procure additional military resources. Governor Janet Napolitano of Arizona, for example, sent the DOD a request for federal funding to support the state's deployment of National Guard troops to the border after reportedly exhausting available state resources for combating illegal immigration and drug trafficking.[2] Others view the increased presence of military support along the borders as undiplomatic, potentially dangerous,[3] and a further strain on already overextended military resources.[4] Nonetheless, the concerns over aliens and smugglers exploiting the porous southern border continue to grow, and some now argue that the military should play a much larger and more direct role in border security.

On May 15, 2006, President Bush announced that up to 6,000 National Guard troops would be sent to the southern border to support the Border Patrol. According to the President, the Guard will assist the Border Patrol by operating surveillance systems, analyzing intelligence, installing fences and vehicle barriers, building roads, and providing training.[5] Guard units will not be involved in direct law-enforcement activities and will be under the control of the Governors.[6] The Administration has indicated that the vast majority of the force at the border would be drawn from Guardsmen performing their regularly scheduled, two- or three-week, annual training, pursuant to Title 32 of the U.S. Code (see later discussion).[7] In Congress, the Senate passed an

amendment (S.Amdt. 4076) to the Comprehensive Immigration Reform Act of 2006 (S. 2611) that would allow the Governor of a state, with the approval of the Secretary of Defense, to order units of the National Guard of such state to perform specified activities (e.g., reconnaissance, training, construction) during annual training duty along the southern land border for border security purposes. Section 1026 of the House-passed Defense Authorization Act for FY2007 (H.R. 5122) would allow the Secretary of Defense, upon a request of the Secretary of DHS, to assign members of the armed forces to assist DHS officials in preventing the entry of terrorists, drug traffickers, and illegal aliens.[8]

Military Assistance along the Border

The military does not appear to have a direct legislative mandate to protect or patrol the border or to engage in immigration enforcement. Indeed, direct military involvement in law enforcement activities without proper statutory authorization might run afoul of the Posse Comitatus Act.[9] The military does have, however, general legislative authority that allows it to provide *support* to federal, state, and local law enforcement agencies (LEA) in counterdrug and counterterrorism efforts, which might indirectly provide border security and immigration control assistance. Military personnel for these operations are drawn from the active and reserve forces of the military and from the National Guard.

Restrictions

The primary restriction on military participation in civilian law enforcement activities is the Posse Comitatus Act (PCA).[10] The PCA prohibits the use of the Army and Air Force to execute the domestic laws of the United States except where expressly authorized by the Constitution or Congress. The PCA has been further applied to the Navy and Marine Corps by legislative and administrative supplements. For example, 10 U.S.C. §375, directs the Secretary of Defense to promulgate regulations forbidding the direct participation "by a member of the Army, Navy, Air Force, or Marines in a search, seizure, arrest, or other similar activity" during support activities to civilian law enforcement agencies. DOD issued Directive 5525.5, which outlines its policies and procedures for supporting federal, state, and local LEAs. According to the Directive, the following forms of direct assistance are prohibited: (1) interdiction of a vehicle, vessel, aircraft, or other similar activity; (2) a search or seizure; (3) an arrest, apprehension, stop and frisk, or similar activity; and (4) use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. It is generally accepted that the PCA does not apply to the actions of the National Guard when not in federal service.[11] As a matter of policy, however, National Guard regulations stipulate that its personnel are *not*, except for exigent circumstances or as otherwise authorized, to directly participate in the arrest of suspects, conduct searches of suspects or the general public, or become involved in the chain of custody for any evidence.[12]

Authorizations

The PCA does not apply "in cases and under circumstances expressly authorized by the Constitution." Under the Constitution, Congress is empowered to call forth the militia to execute the laws of the Union.[13] The Constitution, however, contains no provision expressly authorizing the President to use the military to execute the law. The question of whether the constitutional exception includes instances where the President is acting under implied or inherent constitutional powers is one the courts have yet to answer. DOD regulations, nonetheless, do assert two constitutionally based exceptions — sudden emergencies and protection of federal property.[14] The PCA also does not apply where Congress has expressly authorized use of the

military to execute the law. Congress has done so in three ways: by giving a branch of the armed forces civilian law enforcement authority (e.g., the Coast Guard), by addressing certain circumstances with more narrowly crafted legislation,[15] and by establishing general rules for certain types of assistance.

The military indirectly supports border security and immigration control efforts under general legislation that authorizes the armed forces to support federal, state, and local LEAs. Since the early 1980s, Congress has periodically authorized an expanded role for the military in providing support to LEAs. Basic authority for most DOD assistance was originally passed in 1981 and is contained in Chapter 18 of Title 10 of the U.S. Code — Military Support for Civilian Law Enforcement Agencies. Under Chapter 18 of Title 10, Congress authorizes DOD to share information (§371); loan equipment and facilities (372); provide expert advice and training (§373); and maintain and operate equipment (§374). For federal LEAs, DOD personnel may be made available, under §374, to maintain and operate equipment in conjunction with counterterrorism operations (including the rendition of a suspected terrorist from a foreign country) or the enforcement of counterdrug laws, immigration laws, and customs requirements. For any civilian LEA, §374 allows DOD personnel to maintain and operate equipment for a variety of purposes, including aerial reconnaissance and the detection, monitoring, and communication of air and sea traffic, and of surface traffic outside the United States or within 25 miles of U.S. borders, if first detected outside the border. Congress placed several stipulations on Chapter 18 assistance, e.g., LEAs must reimburse DOD for the support it provides unless the support "is provided in the normal course of military training or operations" or if it "results in a benefit...substantially equivalent to that which would otherwise be obtained from military operations or training."[16] Pursuant to §376, DOD can only provide such assistance if it does not adversely affect "the military preparedness of the United States." Congress incorporated posse comitatus restrictions into Chapter 18 activities in §375.

In 1989, Congress began to expand the military's support role. For example, Congress directed DOD, to the maximum extent practicable, to conduct military training exercises in drug-interdiction areas, and made the DOD the lead federal agency for the detection and monitoring of aerial and maritime transit of illegal drugs into the United States.[17] Congress later provided additional authorities for military support to LEAs specifically for counterdrug purposes in the National Defense Authorization Act for FY1991.[18] Section 1004 authorized DOD to extend support in several areas to any federal, state, and local (and sometimes foreign) LEA requesting counterdrug assistance. This section has been extended regularly and is now in force through the end of FY2006.[19]

As amended, §1004 authorizes the military to: maintain, upgrade, and repair military equipment; transport federal, state, local, and foreign law enforcement personnel and equipment within or outside the U.S.; establish bases for operations or training; train law enforcement personnel in counterdrug activities; detect, monitor, and communicate movements of air, sea, and surface traffic outside the U.S., and within 25 miles of the border if the detection occurred outside the U.S.; construct roads, fences, and lighting along U.S. border; provide linguists and intelligence analysis services; conduct aerial and ground reconnaissance; and establish command, control, communication, and computer networks for improved integration of law enforcement, active military, and National Guard activities. Section 1004 incorporates the posse comitatus restrictions of Chapter 18.[20] Unlike Chapter 18, however, this law does allow support which could affect military readiness in the short-term, provided the Secretary of Defense believes the support outweighs such short-term adverse effect.

The National Guard

The National Guard is a military force that is shared by the states and the federal government and often assists in counterdrug and counterrrorism efforts. After September 11, for example, President Bush deployed roughly 1,600 National Guard troops for six-months under Title 10 authority to support federal border officials and provide a heightened security presence.[21] Under "Title 10 duty status," National Guard personnel operate under the control of the President, receive federal payand benefits, and are subject to the PCA.[22] Typically, however, the National Guard operates under the control of state and territorial Governors. In "state active duty" National Guard personnel operate under the control of their Governor, are paid according to state law, can perform activities authorized by state law, and are *not* subject to the restrictions of the PCA.

Because border security is primarily a federal concern, states, such as Arizona, have looked to the federal government for funding to support some of their National Guard activities. Under Title 32 of the U.S. Code, National Guard personnel generally serve a federal purpose and receive federal pay and benefits, but command and control remains with the Governor. This type of service is commonly referred to as "Title 32 duty status," and examples are discussed below. The deployment of the 6,000 Guardsmen might be derived from one or more of the authorities listed below. However, because the National Guard are supposed to be performing their border activities during their annual training duty, authority may also stem from 32 U.S.C. §502(a) — the authority that allows the Secretary of the Army and Air Force to prescribe regulations for National Guard drill and training.

State Drug Plan

Federal funding may be provided to a state for the implementation of a drug interdiction program in accordance with 32 U.S.C. §112. Under this section, the Secretary of Defense may grant funding to the Governor of a state who submits a "drug interdiction and counterdrug activities plan" that satisfies certain statutory

However, it appears that the National Guard could be deployed by the President under 10 U.S.C. §§331-333 and §12406 to "execute the laws of the United States." requirements. The Secretary of Defense is charged with examining the sufficiency of the drug interdiction plan and determining whether the distribution of funds would be proper. While the emphasis is certainly on counterdrug efforts, a state plan might include some related border security and immigration-related functions that overlap with drug interdiction activities. Arizona's drug interdiction plan, for example, recognizes related border issues created by human smuggling and terrain vulnerabilities with respect to the illegal entry of aliens into the United States.[23] By approving the State of Arizona's drug interdiction plan, the Secretary of Defense has enabled the Arizona National Guard to engage in some border security measures.

Other Duty

Section 502(f) of Title 32 has been used to expand the operational scope of the National Guard beyond its specified duties. This provision provides that "a member of the National Guard may... without his consent, but with the pay and allowances provided by law...be ordered to perform training *or other duty*" in addition to those they are already prescribed to perform (emphasis added). This is the provision of law which was used to provide federal pay and benefits to the National Guard personnel who provided security at many of the nation's airports after September 11, and who participated in Katrina and Rita-related disaster relief operations. States, such as

Arizona, have argued that the "other duty" language should be liberally applied (like it was for Hurricane Katrina and Rita) to include activities associated with border security efforts.[24] Some question, however, whether domestic operations, in general, are a proper use of this Title 32 authority.[25]

Homeland Defense Activity

In 2004, Congress passed another law that could arguably provide federal funding for National Guard personnel conducting border security operations under Title 32.[26] Chapter 9 of Title 32 of the U.S. Code authorizes the Secretary of Defense to provide federal funding at his discretion to a state, under the authority of the Governor of that state, for the use of their National Guard forces if there is a "necessary and appropriate" "homeland defense activity."[27] A "homeland defense activity" is statutorily defined as "an activity undertaken for the military protection of the territory or domestic population of the United States ... from a threat or aggression against the United States." Although a deployment of National Guard troops for border security purposes could arguably be an activity "undertaken for the military protection" of a "domestic population," it is unclear whether the porous nature of the border or illegal entry of aliens is the type of "threat" or "aggression" that would be "necessary and appropriate" for National Guard troops. The State of Arizona has requested federal funds for its National Guard under Chapter 9 for the performance of homeland defense-border security activities.

End notes

1. Dep't. of Defense, Strategy for Homeland Defense and Civil Support, at 5 (June 2005) available at [http://www.fas.org/irp/agency/dod/homeland.pdf].

2. See [http://azgovernor.gov/dms/upload/NR_030706%20Rumsfeld_Chertoff%20Letter.pdf].

3. In 1997, a Marine who was part of a four-man border observation team near Redford, Texas, shot and fatally wounded an 18-year old man after reportedly taking fire. See *Oversight Investigation of the Death of Esequiel Hernandez, Jr.,* A Report of Chairman Lamar Smith to the Subcommittee on Immigration and Claims of the Committee on the Judiciary, 105th Cong. 2d Sess. (Nov. 1998).

4. Peter Baker, *Bush Set to Send Guard to Border,* THE WASHINGTON POST, May 15, 2006.

5. Stephen Dinan, *Bush Calls for Guard on Border,* THE WASHINGTON TIMES, May 16, 2006.

6. Id.

7. The White House, Press Briefing on the President's Immigration Reform Plan, May 16, 2006, available at [http://www.whitehouse.gov/news/releases/2006/05/20060516-2.html].

8. H.R. 1986, H.R. 3938, H.R. 3333, and H.R. 4437 would propose similar measures.

9. For a more complete discussion of the Posse Comitatus Act, see CRS Report 95-964, *The Posse Comitatus Act & Related Matters: The Use of Military to Execute Civilian Law,* by Charles Doyle.

10. 18 U.S.C. §1385.

11. See CRS Report 95-964, at 42 (citing numerous cases); see also DOD Directive 5525.5.

12. NGR 500-2/ANGI 10-801, *National Guard Counterdrug Support,* March 31, 2000.

13. U.S. Const. Art. I, §8, cl. 15. In addition, the PCA does not apply to actions furthering a military purpose. See CRS Report 95-964, at 31 (describing the exception).

14. 32 C.F.R. §215.4.

15. See, e.g., 10 U.S.C. §§ 331-333 (to suppress insurrections).

16. 10 U.S.C. §377.

17. National Defense Authorization Act for FY1990 and 1991, P.L. 101-189, Div. A, Tit. XII, §1202(a)(1), codified at 10 U.S.C. §124. A similar provision was first passed as part of the National Defense Authorization for FY1989 (P.L. 100-456), but was repealed by P.L. 101-189.

18. P.L. 101-510, Div. A, Tit. X, §1004, codified at 10 U.S.C. §374 note.

19. P.L. 107-107, Div. A, Tit. X, §1021 (extending §1004 through FY2006).

20. Id. at §1021(g).

21. Maj. Gen. Timothy J. Lowenberg, The Role of the National Guard in National Defense and Homeland Security, (Sept. 2005) available at [http://www.findarticles.com/p/articles/mi_qa3731/is_200509/ai_n15638615/print] [hereinafter Lowenberg, The Role of the National Guard].

22. 10 U.S.C. §§12301-12304.

23. State of Arizona, Press Release, Title 32: Statutory Funding Options (Mar. 6, 2006) [http://azgovernor.gov/dms/upload/NR_030906_%20Border%20Veto%20Legal%20Support %20Letter.pdf].

24. Id.

25. Lowenberg, The Role of the National Guard.

26. Defense Authorization Act for Fiscal Year 2005, P.L. 108-375, Div. A, Tit. V, Subtitle B, §§901-908.

27. 32 U.S.C. §905.

Note: This article was originally published in the 23 May 2006 edition of *CRS Report for Congress.*

Defend the United States and Support Civil Authorities at Home

Reprinted with permission from *Quadrennial Defense Review.*

The first responsibility of any government and its defense establishment is to protect the lives and safety of its people. Because the United States benefits from favorable geography and continental size, direct attacks against the country itself have been rare throughout our history. However, events since the terrorist attacks of September 11, 2001, remind us that the rapid proliferation of destructive technologies, combined with potent ideologies of violent extremism, portends a future in which all governments will have to maintain a high level of vigilance against terrorist threats. Moreover, state adversaries are acquiring new means to strike targets at greater distances from their borders and with greater lethality. Finally, the United States must also be prepared to respond to the full range of potential natural disasters.

The experiences of the past several years have deepened the realization that state- and non-state adversaries alike may seek to attack military and civilian targets within the United States. Protecting the nation and its people from such threats requires close synchronization between civilian and military efforts. Although many efforts to protect the United States are led by other federal agencies, including the Department of Homeland Security (DHS), the role of the Department of Defense in defending the nation against direct attack and in providing support to civil authorities, potentially in response to a very significant or even catastrophic event, has steadily gained prominence.

When responding to an event within the United States, the Department of Defense (DoD) will almost always be in a supporting role. DoD can receive requests to provide federal assistance through two avenues: first, through DHS as the lead federal agency, or second, through a governor's request under U.S. Code Title 32 authorities.

To ensure that the Department of Defense is prepared to provide appropriate support to civil authorities, the QDR examined the sufficiency of the programmed force and sought to identify capability enhancements that were of highest priority for the future. Key initiatives resulting from this assessment include efforts to:

- **Field faster, more flexible consequence management response forces.** The Department has gained important experience and learned valuable lessons from its efforts to field specialized consequence management response forces for chemical, biological, radiological, nuclear, and high-yield explosives events (CBRNE). Given the potential for surprise attacks within the United States, the Department will begin reorganizing these forces to enhance their lifesaving capabilities, maximize their flexibility, and reduce their response times. First, the Department will begin restructuring the original CBRNE Consequence Management Response Force (CCMRF), to increase its ability to respond more rapidly to an event here at home. To address the potential for multiple, simultaneous disasters, the second and third CCMRFs will be replaced with smaller units focused on providing command and control and communications capabilities for Title 10 follow-on forces. Complementing the evolution of the first CCMRF, the Department also will draw on existing National Guard forces to build a Homeland Response Force (HRF) in each of the ten Federal Emergency Management Agency (FEMA) regions. These ten HRFs will provide a regional response capability; focus on planning, training and exercising; and forge strong links between the federal level and state and local authorities.

- **Enhance capabilities for domain awareness**. The Department of Defense and its interagency partners must be able to more comprehensively monitor the air, land, maritime, space, and cyber domains for potential direct threats to the United States. Such monitoring provides the U.S. homeland with an extended, layered in depth defense. This effort includes enhanced coordination with Canada for the defense of North America as well as assisting Mexico and Caribbean partners in developing air and maritime domain awareness capacities. Special attention is required to develop domain awareness tools for the Arctic approaches as well. In coordination with domestic and international partners, DoD will explore technologies that have the potential to detect, track, and identify threats in these spheres to ensure that capabilities can be deployed to counter them in a timely fashion. For example, the Department is working with DHS and the Defense Intelligence Agency (DIA) through a joint technology capability demonstration program to explore new technologies to assist in the detection of tunnels. This technology can support U.S. authorities conducting domestic missions and also help meet the needs of forces operating overseas.

- **Accelerate the development of standoff radiological/nuclear detection capabilities**. DoD will improve its ability to detect radiological and nuclear material and weapons at a distance. Developing and fielding these sensors will make possible more effective wide area surveillance in the maritime and air approaches to the United States, and will help address the challenge of locating and securing nuclear weapons and materials during overseas contingencies.

- **Enhance domestic counter-IED capabilities.** To better prepare the Department to support civil authorities seeking to counter potential threats from domestic improvised explosive devices (IEDs), DoD will assist civil authorities with counter-IED tactics, techniques, and procedures (TTPs) and capabilities developed in recent operations.

Note: This article was originally published in the Feb. 2010 edition of *Quadrennial Defense Review.*

Section 2: Coordinated Efforts of Border Security

How the Military Supports Homeland Security

General Gene Renuart, U.S. Air Force

In my capacity as Commander of U.S. Northern Command (USNORTHCOM), I am also Commander of the North American Aerospace Defense Command (NORAD) and the counterpart to the Commander of Canada Command (Canada COM), our partner to the north. These three organizations have complementary missions in protecting our homelands, and they work together closely.

NORAD—a more than 51-year-old bi-national U.S.-Canadian command governed by the *NORAD Agreement*—is responsible for aerospace warning and control and the relatively new and developing mission of maritime warning for the two countries. NORAD ensures U.S. and Canadian air sovereignty through a network of alert fighters, tankers, airborne-early-warning aircraft, and ground-based air-defense assets cued by interagency and defense surveillance systems.

USNORTHCOM, a unified combatant command established on 1 October 2002, has the joint missions of homeland defense—incorporating maritime defense, plus missile defense of the homeland—and defense support of civil authorities (DSCA).

Both commands share headquarters staff and use the same consolidated command center. And USNORTHCOM's civil authorities support work reinforces the Department of Homeland Security (DHS), among other agencies.

Multiple Domains

Operating in a variety of domains, USNORTHCOM must prepare for homeland defense and DSCA in each simultaneously. The air, space, land, maritime, and cyber domains can all be affected by natural disasters or man-made threats and certainly each can have an impact on the others.

For example, the maritime domain can be affected by threats from the air, cyberspace, and the sea. If we can be attacked in all of these by man or Mother Nature, then we must defend against or at least mitigate the threat in each of them. Our goal and role is to ensure that the Department of Defense is properly positioned to do that—leading if it's a case of military homeland defense, supporting DHS if it's a case of homeland security, and working effectively with DHS and its components in operational situations that require transition between homeland defense and security, which certainly can happen.

Threats to our homeland have obviously changed in this new century. As DHS Secretary Janet Napolitano noted on 30 July 2009: "We cannot forget that the 9/11 attackers conceived of their plans in the Philippines, planned in Malaysia and Germany, recruited from Yemen and Saudi Arabia, trained in Pakistan and Afghanistan, and carried them out in the United States." Of course, much of our homeland defense and security effort is focused overseas. Thus, we conduct a daily counterterrorism video conference with U.S. Central Command and others. Our view must be global, in all domains.

Progress—It's About Teamwork

We are committed to support the many components of DHS and other federal agencies, when requested and directed by the President or Secretary of Defense. In fact, I spend a lot of time on Capitol Hill advocating for resources needed by other federal agencies and for our partners in the National Guard. Speaking about the significance of soft power to our country, Secretary of Defense Robert Gates mentioned the importance of investing more in the Departments of State, Agriculture, Justice, and other government agencies that can provide the reconstruction capacity we need in some of our overseas operations.

The same is true for us in the homeland. Under the *National Response Framework*, DOD must be prepared as a supporting agency for every single emergency support function. So it is important to us that DHS and other primary agencies for the various emergency support and federal law enforcement functions be adequately funded so they can carry out their border-security, maritime-surveillance, intelligence-fusion, and disaster-response roles.

This is especially crucial in certain homeland security functions for which we in DOD are not organized, trained, or equipped. But we also know that terrorists and Mother Nature don't exactly create disasters for which the pre-planned response at every level of government is predictably perfect and with unlimited resources. So we make ourselves ready, if needed, as quiet professionals capable of making a difference and doing it in support of state governors and federal agencies.

National Guard, Reserve, and Other Agencies

In our headquarters, nearly 10 percent of USNORTHCOM's full-time military staff draws from the National Guard and Reserve, who bring strong experience from the states. We have 52 different federal agencies represented in or near our headquarters every day. These are senior representatives provided by their agencies to work directly in our planning and emergency operations. They include people from the State Department and the Federal Aviation Administration, along with DHS and many of its elements, i.e., the Federal Emergency Management Agency (FEMA), the Transportation Safety Administration, and the Coast Guard.

BILATERAL MILITARY PLAN In February 2008, the author (left) and Canadian air force lieutenant general Marc Dumais, commander of Canada command, signed a Civil Assistance Plan that allows the military from one nation to support the armed forces of the other during a civil emergency. "This provides the technical avenue through which we can help each other quickly," the author says.

We also have liaison officers from other combatant commands and an FBI representative who briefs me routinely on counterterrorism operations. We, in turn, have two action officers at the National Counterterrorism Center and another in the FBI's National Joint Terrorism Task Force, plus officers in various parts of DHS, other unified commands, the National Guard Bureau and Canada Command, as well as a Washington office.

After Hurricane Katrina, we placed a defense coordinating officer, with a supporting defense coordinating element, in each of the FEMA regions. This team helps plan for the kinds of events that can occur in each particular region, so that we can be prepared to provide tailored support when it's required, requested, and directed.

In addition to our interagency associates, we have great international partners. Nearly 130 Canadians are in our headquarters, primarily focused on NORAD air, space, and now maritime-warning operations, but also integrated into our strategy and plans, logistics, policy, and intelligence cells. We share mutual support with our partners in Canada Command through a bilateral *Civil Assistance Plan* that we signed in February 2008. This provides the technical avenue through which we can help each other quickly, as when a Canadian C-17 airlifted American medical patients before Hurricane Gustav came ashore last year. It worked very well.

Finally, just as the Department of State and DHS have cooperative programs with counterpart Mexican government agencies, our theater security cooperation activities extend to our friends in the armed forces of Mexico—with whom I think we enjoy the best relationships we've ever had. In our headquarters, senior Mexican Navy and Air Force liaison officers serve to support the Mexican government in its fight against the drug cartels, which helps make our homeland safer.

Maritime Collaboration

The relationship we have with our Sea Service partners is strong. We've built an interagency team that can collaborate smoothly, train together, and operate effectively. Routinely, we have Coast Guard or FBI officers on board our Navy ships to support maritime law enforcement when they ask for Navy assistance. NORAD, USNORTHCOM, the Navy, and the Coast Guard collaborate in many homeland-defense operations. For example, our air defense of the National Capital Region includes Coast Guard helicopters, with crews trained to do airborne intercept that helps us vector away aircraft infringing on restricted air space.

COLLABORATION WITH MEXICO Mexican Navy and Air Force liaison officers serve at USNORTHCOM headquarters to support their country's fight against drug cartels. Here, U.S. First Air Force commander Major General Hank Morrow (left) discusses North American homeland operations with Major General Carlos Antonio Rodriquez Munguia, deputy director of operations for the Mexican Air Force.

We also partner in mine countermeasures activity. As an Air Force fighter pilot, I never thought much about the bottoms of ports. But I have learned that over time, tides, storms, and other events change their structure. It is nice to know what's there so that if we do get intelligence of a new maritime explosive device here in our homeland, we can understand what's already under the water in our ports and quickly survey to see what's different. With interagency cooperation and key Navy and Coast Guard roles, as a team we're completing these important port surveys.

We have just over 30 Coast Guardsmen (active duty and reserve) fully integrated into our staff, including an outstanding USNORTHCOM Deputy Director of Operations. We're engaged with the Coast Guard's Pacific and Atlantic area commands, and we're very supportive as that service realigns itself into an operational command structure. We're also integrated into each other's maritime planning and execution processes. For example, NORTHCOM served as DOD lead, teamed with the Coast Guard as DHS lead, in co-writing the national *Maritime Domain Awareness Concept of Operations.*

With Canada Command, we're pursuing development of a *Canada-U.S. Maritime Defense Plan.* Supporting the Navy lead in the DOD Maritime Domain Awareness campaign, USNORTHCOM is the lead operational manager for technology demonstration projects, entitled *Comprehensive Maritime Awareness* and *Maritime Automated Super Track Enhanced Reporting,* and we teamed with the U.S. Pacific Command to develop the *Maritime Domain Awareness Joint Integrating Concept.* We've participated in the coordination of a DHS-Department of Transportation-DOD interagency memorandum of agreement to guide U.S. Government participation in the international Maritime Safety and Security Information System. Our two major annual USNORTHCOM exercises, Ardent Sentry and Vigilant Shield, foster vigorous collaboration among interagency and international maritime and law-enforcement organizations, a strong team effort that gets better each year.

Within our headquarters we've established a private-sector office that works closely with its DHS and FEMA counterparts. The maritime industry plays a big role in national security, and the private sector is a huge part of maritime security around the world, just as it owns and operates the vast majority of American transportation and critical infrastructure. So we've looked for ways to partner with private-sector shipping companies, pilots' associations, and others to help us create shared situational awareness of what's in the domain so we can, in my words, "sort the friendlies." Having to look at two or three vessels of concern is a lot better than having to sort through 200.

Unity of Effort

Homeland defense and security and disaster preparedness and response require team play at all levels. With this in mind, we at USNORTHCOM are constantly focused on communication, coordination, collaboration, and integration. Traditional military unity of command is key to successful military operations—including DSCA operations. But the term doesn't fit very well into a whole-of-government, interagency federal/state/local/tribal, private-sector *National Response Framework* lexicon, which is about collaborative unity of effort.

Each of our partners at these levels is unique. They have their own authorities, usually mandated by law. This includes the private sector. Nowhere in law does it say that DOD is in command of any civil law enforcement agencies. Posse Comitatus prohibits it, and we are especially sensitive not to step outside those guidelines. Our role in homeland security is to build confidence among our partners and be there in support when they ask for it, bringing capabilities and capacities that DOD can provide to help our to protect our citizens.

Teaming with others begins with building relationships. We work closely every day with our civilian partners, agencies like DHS, Health and Human Services, FBI, and the Drug Enforcement Agency, as well as the private sector. Since she's been in office, Secretary Napolitano and I have created a relationship that allows us to be successful as a team, with

USNORTHCOM in support of DHS. This is critical when the nation comes under the stress of a natural or manmade disaster. We host a biweekly, informal Interagency Planner Synchronization Working Group at the national level. We actively participate in the DHS-led Integrated Planning System, and in the National Exercise Program. We do our best to integrate planning, training exercises, and responses—not only of joint DOD forces, or of Title 10 and National Guard forces on state duty, or of combined U.S. and foreign forces (as with Hurricanes Katrina and Gustav), but with all of our civilian partners. We have to be able to do that under stress. It's not smart to start exchanging business cards at the scene of a disaster. This begins with building trusted, knowledgeable working relationships before disaster happens—one of the most important things we do every day.

Homeland Defense Support of Civil Authorities

We provide support to other agencies during unique and varied operations like the Presidential inauguration, the United Nations General Assembly, G-20 and other summits, the Super Bowl, the Democratic and Republican National Conventions, space shuttle launches, and wild land firefighting wherever required and requested by civilian officials around the country. There's annual flooding in the Midwest and elsewhere, with which we can be asked to help, in addition to the Army Corps of Engineers' separate authorities, responsibilities, and appropriations as established by law.

In response to the I-35 bridge collapse in Minneapolis back in August of 2007, USNORTHCOM provided Navy salvage divers to go in and recover the remains of people killed—in support of the Department of Transportation, which was supporting the local sheriff. We did that deployment in a few hours after being tasked, with just a few phone calls. One of the reasons we monitor events around the country, anticipate potential requests, and lean forward to prepare, is so we don't have a cold start and can respond quickly.

We support civil agencies that do counter-drug and border-security operations of many kinds, including legally authorized tunnel detection and logistical and sensor support to law enforcement agency interdiction of illegal trafficking. We also support and conduct environmental response. We have to understand how the other partners operate, and how we can integrate our support with them. For example, last year after Hurricanes Gustav and Ike, we used Navy sonar towed behind helicopters to help survey the channels into the ports of New Orleans and Galveston to allow for rapid and safe opening of those ports to commercial traffic.

Let's be clear: when supporting civil authorities, we come to a state or a region only on the direction of the President and/or Secretary of Defense, typically when federal support has been requested by a governor, putting the right assets in the right place at the right time. When we're no longer needed, we go away. By law, we can also be directed to support civil law enforcement agencies, especially in their efforts to stop illicit drug smuggling across our borders. But we're *not* doing civil law enforcement.

Our Approach to DSCA

We added a word to our USNORTHCOM mission statement a couple of years ago to imprint it into our culture. If you walk into our command center, you'll see about a 25-foot-wide banner, with 14-inch-tall letters, that says, "Anticipate." If we're not thinking ahead, if we're not planning in advance, then we'll not respond well. And the response will always be later than needed. We'd be slow and clumsy instead of resilient, creative, adaptive, and effective in crisis response.

I-35 BRIDGE COLLAPSE A great example of how USNORTHCOM response is supposed to work took place in August 2007, when Navy salvage divers were dispatched to Minneapolis "within a few hours after being tasked" for the recovery effort. Such preparation and anticipation, the author says, "is so we don't have a cold start and can respond quickly."

That doesn't mean you'll always preclude an event from happening. Mother Nature has a tendency to do things her own way. But if you plan for those kinds of events, if you've built good interagency working relationships, if you've done smart things like working with FEMA in its pre-scripted mission assignments system, then you're much more likely to be ready to mitigate and respond when bad things happen in America. I do not accept the attitude of "stuff happens." It's our job to anticipate and prepare, with the resources we have, under applicable laws and directives.

Every day, our command center monitors 35 to 40 events across North America, including maritime events involving vessels of interest. We need to ensure that each of these events is visible to us, and we anticipate the implications of any one of them turning into a crisis, fortunately, very few do. But if one does, we can be in a position to respond immediately. Our command center shares information with some 150 other command centers in North America. That's a big business for us, and the sharing of information is central to everyone's success.

International friends are key to our homeland defense and security, especially our neighbors here on this continent. A Canadian general was in the NORAD Operations Center directing initial air defense over our homeland as 9/11 unfolded. NATO airborne early warning crews flew in support of NORAD over our homeland after 9/11. The Canadians evacuated American medical patients as Hurricane Gustav approached last year. Mexican Army troops fed displaced Americans after Hurricanes Katrina and Rita, and they are now fighting the drug cartels that

smuggle illegal drugs into the United States. If you tally the deaths, the injuries, and medical costs, and the societal impact of the crime drugs cause, the financial and strategic impact to our nation is huge. As in the neighborhood around your home, you're a lot safer if good neighbors are watching out for you. Canada and Mexico are very important to us.

Present and Future Challenges

My focus, beyond readiness to respond to any homeland crisis, is on the future. We're not just adapting to change, we're working to anticipate and help lead it. Following is a short list of some of the key challenges we're helping to shape now and for the future:

- Maritime Domain Awareness;
- Arctic Presence, Safety, and Security;
- Ballistic- and Cruise-Missile Defense of the Homeland;
- NORAD Aircraft Recapitalization and Radar Sustainment (including Title 10, National Guard, and Canadian assets—as well as FAA radars on which we depend);
- Resourcing and Fielding of Three Nationally-Responsive CBRNE (Chemical, Biological, Radiological, Nuclear, Explosive) Consequence Management Response Forces (CCMRF);
- Theater Security Cooperation with Our North American Neighbors;
- Access to Reserve Forces for National Disaster Response;
- Improving DOD Incident Awareness and Assessment tools for DSCA Missions;
- Collaborative Planning, Training, Exercises and Operations with Federal Interagency and State Partners;
- Defending Our Cyber Networks, plus Roles & Missions Definition for Cyber DSCA;
- Pandemic Readiness (USNORTHCOM is assigned as DOD global pandemic influenza planning lead) and Preparing for Potential Pandemic DSCA Roles.

Our solemn obligation in USNORTHCOM, as in NORAD with Canada, is to defend our homelands. We support civil authorities as part of the larger federal effort, when directed under law. We are volunteers who have sworn to support and defend the Constitution. We're proud to defend our citizens and to support the civil agencies that protect them. Ready now, we're actively anticipating and preparing for a changing future, which we'll help shape as a trusted team player, guarding what you value most.

General Renuart is Commander of U.S. Northern Command and the North American Aerospace Defense Command. He entered the Air Force in 1971 and has logged more than 3,900 flight hours, including 60 combat missions.

Military Homeland Security Support: Joint Task Force North Supports Federal Agencies

Armando Carrasco, Joint Task Force North Public Affairs

Securing the nation and safeguarding citizens are the top priorities for federal law enforcement agencies. Supporting federal homeland security efforts is the mission of Joint Task Force North (JTF North).

JTF North, based at Fort Bliss, Texas, is the Department of Defense (DOD) organization tasked to support federal law enforcement agencies in identifying and interdicting suspected narcotics-related traffickers and other transnational threats. While JTF North's mission authorities are based on counterdrug/counternarcotrafficking federal laws, the task force support operations are executed to counter associated transnational threats. Transnational threats include activities that threaten the national security of the United States, including international terrorism, narcotrafficking, alien smuggling, and threats involving weapons of mass destruction.

JTF North homeland security support missions are executed as part of the DOD's military support to civilian law enforcement agencies (MSCLEA) responsibilities. The homeland security support provided by JTF North is designed to enhance law enforcement agencies' efforts to anticipate, detect, deter, prevent, and defeat transnational threats to the homeland.

Joint Task Force North Mission: JTF North provides military support to law enforcement agencies, conducts theater security cooperation as directed, and facilitates interagency synchronization within the U.S. Northern Command (USNORTHCOM) area of responsibility in order to anticipate, detect, deter, prevent, and defeat transnational threats to the homeland.

As a subordinate element of USNORTHCOM, JTF North is under the operational control of U.S. Army North, the joint force land component command. The task force operates within the USNORTHCOM area of responsibility, which encompasses the entire North American continent, to include the air, land, and sea approaches.

Requests for Military Support

When domestic law enforcement agencies request DOD operational or other types of support from JFT North, DOD policy requires the requests to first be offered to the appropriate state National Guard (NG) counterdrug coordinator to determine whether the state NG can provide the support. To accomplish this requirement, the NG Bureau maintains a liaison team within the JTF North headquarters. If a determination is made that the NG does not have the requested support capabilities or available assets, the request is considered by JTF North.

All support requests submitted to JTF North must comply with U.S law and DOD policy for domestic employment of Title 10, U.S. Code, federal military forces. During the first decade of JTF North's MSCLEA operations, the support provided to law enforcement was relatively personnel intensive, using people on the ground to provide border detection. Today, JTF North support has shifted to a greater focus on the application of technologies, including ground sensors, radar, airborne platforms, and thermal imaging.

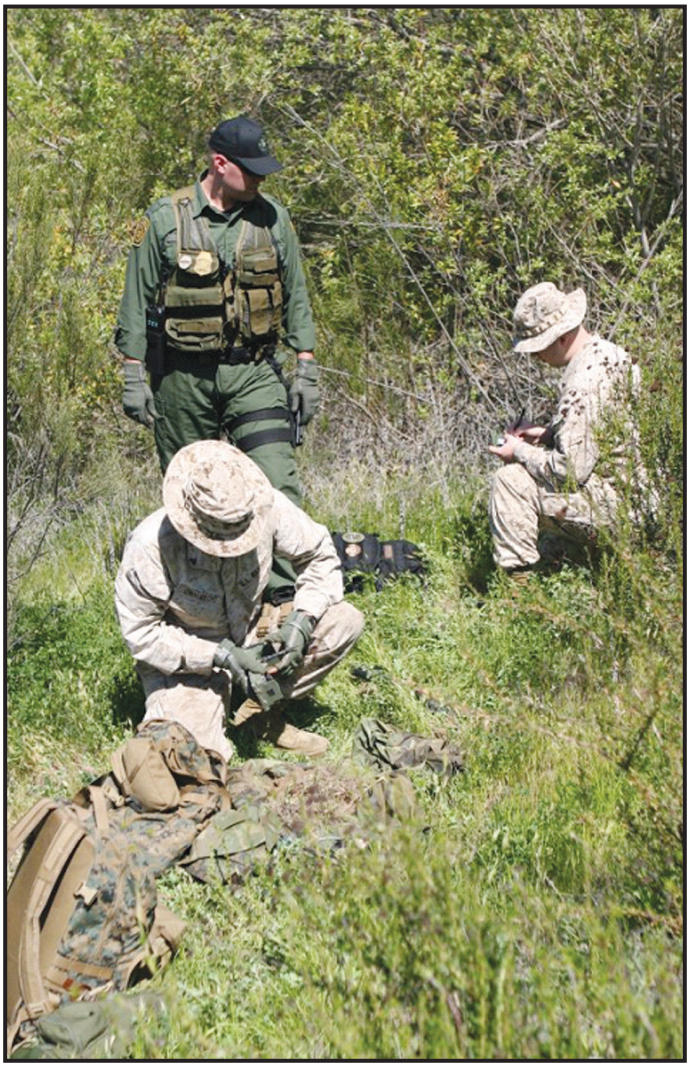


Figure 1. An agent from U.S. Border Patrol–San Diego Sector maintains security while Marines from the 4th Ground Sensor Platoon, Intelligence Support Battalion, install ground sensors in a remote area along the U.S.-Mexico border.

Figure 2. Marine Medium Helicopter Squadron-764 airlifted U.S. Border Patrol–San Diego Sector air mobile unit agents and their all-terrain vehicles to remote mountainous locations along the U.S.-Mexico border.

The evolution of the support has resulted in more effective border detection. JTF North has shifted its intelligence support efforts from the borders outward and deeper into the approaches to the United States. Working more closely with Canadian and Mexican agencies, JTF North is gaining greater visibility on threats as they enter the USNORTHCOM area of responsibility. The end result is an increased ability to alert partner nations working in cooperation with U.S. law enforcement to interdict the threats before they reach the United States.

Military Volunteers Perform Support Missions

As an operational planning headquarters, JTF North is comprised of 180 active duty and reserve component Soldiers, Sailors, Airmen, Marines, Coast Guardsmen, DOD civilian employees, and contracted support personnel. The joint service command, which has no assigned forces, relies on volunteer Title 10 active duty and reserve component units and individual military assets to accomplish its homeland security support mission.

JTF North solicits volunteer units from each of the four DOD branches. The volunteer units must be equipped with the appropriate military skills and capabilities required to perform the requested operational support missions. The Title 10 units and personnel executing the JTF North support missions operate under the tactical control of the JTF North commander. In its continued effort to synchronize the JTF North support missions, the task force routinely coordinates its support operations with other DOD support assets, including the NG.

Figure 3. Soldiers from the 1st Squadron, 6th Air Cavalry Regiment unload an OH-58D Kiowa Warrior helicopter deployed to the U.S.-Mexico border via a U.S. Air Force C-5 Galaxy aircraft. The Soldiers employed their forward-looking infrared (FLIR) equipped aircraft while conducting aviation reconnaissance operations in support of the U.S. Border Patrol–El Paso Sector.

Figure 4. The JTF North intelligence directorate, geospatial intelligence office, provides volunteer military units, supported law-enforcement agencies, and the JTF North staff with imagery support, including multiple scale maps, line drawings, and custom geospatial intelligence analyses.

Figure 5. Seabees from Naval Mobile Construction Battalion 24 constructed low-water crossings, fences, and roads along the U.S.-Mexico border near Douglas, Arizona in support of the U.S. Border Patrol–Tucson Sector.

The volunteer units must comply with legal and policy guidelines, including the Posse Comitatus Act and intelligence oversight policies. Based on U.S. law, the active duty and reserve component military forces can only be employed to provide support. They are strictly prohibited from being used in a direct law enforcement role.

Once a unit volunteers for a specific mission, JTF North facilitates mission planning and execution with the unit and the supported agency. Field grade officers and senior noncommissioned officers are assigned as mission planners to assist the volunteer units in mission preparation and to facilitate coordination with the federal law enforcement agencies. Mission planners ensure that each operation is conducted legally, efficiently, and safely. JTF North also operates a 24-hour joint operations coordination center to resolve and coordinate issues that the volunteer military units may encounter.

Under DOD policy, the approved support missions must either provide a training benefit to the unit or make a significant contribution to national security. The JTF North missions provide volunteer units with real-world training opportunities that directly increase their combat effectiveness. While supporting law enforcement agencies, volunteer units typically train in 90 percent of wartime mission tasks. Many of the volunteer active duty and reserve units have used JTF North missions as train-up opportunities before deploying to Iraq or Afghanistan. To prepare for future deployments, some units returning from Iraq and Afghanistan volunteer for additional JTF North missions.

Units executing JTF North missions along the southwest border areas also gain the added benefit of conducting concurrent unit training at some of the best training ranges in the world, including the Fort Bliss training ranges, Arizona's Goldwater Range, and the Yuma Proving Ground.

JTF North missions truly yield win-win situations: the volunteer units gain great training opportunities and the nation's law enforcement agencies get much needed support.

While the task force can respond to short-notice support requests, most mission planning takes several weeks or many months, depending on each mission's requirements. Actual mission duration can vary from a couple of weeks to several months.

Categories of Military Support

JTF North support to federal law enforcement agencies is categorized in the following six support categories and listed types of support:

- Operational support.
    - Aviation support operations.
        - Aviation transportation/insertion/extraction.
    - Aviation reconnaissance.
        - Daytime operations.
        - Nighttime operations.
    - Air and maritime surveillance radar.
    - Unmanned aircraft systems.
    - Ground surveillance radar.
    - Listening post/observation post.
    - Ground sensor operations.
    - Ground transportation.
- Intelligence support.
    - Collaborative threat assessment.
    - Geospatial intelligence support.
    - Modified threat vulnerability assessment.
    - Threat link analysis product.

- Engineering support (only within the southwest border).
    - Personnel barriers.
    - Vehicle barriers.
    - Lights.
    - Roads.
    - Bridges.
- General Support.
    - Mobile training teams.
        * Basic marksmanship.
        * Trauma management.
        * Emergency response.
        * Counterdrug field tactical police operations.
        * Counterdrug marksman/observer training.
        * Counterdrug special reaction team training.
        * Integrated mission planning.
        * Intelligence and link analysis.
        * Interview techniques.
        * Multisubject tactical instruction.
        * Threat mitigation training.
        * Other training as requested.
    - Tunnel detection.
    - Transportation.
    - Sustainment.

Figure 6. JTF North executed a multisensor land and maritime homeland security mission in support of the U.S. Coast Guard along the U.S.-Mexico border south of San Diego. The support mission included both day and night aviation reconnaissance and maritime radar support operations.

Figure 7. A 94th Engineer Battalion safety noncommissioned officer discusses a JTF North border-road mission with a U.S. Border Patrol agent providing security for the military engineers. The Fort Leonard Wood engineers constructed approximately one mile of improved roads and several low-water crossings in Laredo, Texas near the U.S.-Mexico border.

- Interagency synchronization.
    - Support interagency planning process.
    - Facilitate interagency and binational information sharing.
    - Leverage point of integration operations (multi-agency, multi-assets operation).

- Technology integration.
    - DOD science and technology investment.
    - Ground/air/maritime sensor integration.
    - Information efficiency and networks.
    - Biometrics.
    - Tunnel detection.

National Guard Support to Law Enforcement

JTF North support missions are executed separately from NG, Title 32, U.S. Code law enforcement support efforts. NG support is provided under the authority of each state's governor. All law enforcement support requests are first offered to the appropriate state NG counterdrug coordinators before they are considered by JTF North.

In order to maximize the total military support effort, JTF North staff routinely works directly with the NG Bureau and the NG Counterdrug Division as well as with state NG joint forces headquarters and counterdrug task forces where JTF North support operations are conducted.

The combined efforts provided by JTF North and the NG serve as enablers that enhance federal law enforcement agencies' capabilities to disrupt and defeat threats to the nation.

The JTF North staff of DOD professionals is committed to accomplishing the command's mission; their dedication to the homeland security support role is best summed up in JTF North's motto: "Service to the Nation." For more information on JTF North, visit the command's Website at <www.jtfn.northcom.mil>.

Joint Task Force North History

- JTF North, formerly known as Joint Task Force–Six (JTF–6), was established in response to President George H.W. Bush's declaration of the war on drugs. General Colin Powell, then commanding general of U.S. Army Forces Command, issued the order that established JTF–6, effective November 13, 1989.
- JTF–6 was established to serve as the planning and coordinating operational headquarters to support local, state, and federal law enforcement agencies within the Southwest border region to counter the flow of illegal drugs into the United States.
- JTF–6's original area of operations consisted of the four border states of California, Arizona, New Mexico, and Texas—a land area of more than 660,000 square miles. In February 1995, by directive of the Commanding General of U.S. Army Forces Command, JTF–6's area of responsibility was expanded to include the entire continental United States, Puerto Rico, and the Virgin Islands.

- JTF–6's efforts led to both a greater recognition of the potential for military assistance in counterdrug efforts and a significant expansion of the partnerships among active duty forces, reserve components, and the nation's law enforcement agencies.

- The tactics, techniques, and procedures that the command developed over the years in the war on drugs contribute immeasurably to the accomplishment of JTF North's new and broader mission of combating transnational threats.

- In a ceremony conducted on September 28, 2004, JTF–6 was officially renamed JTF North.

From its inception as JTF–6 to its evolution as JTF North, the command has completed over 6,000 missions in support of the nation's local, state, and federal law enforcement agencies and counterdrug task forces.

Protecting Our Borders Against Terrorism

Reprinted with permission from the U.S. Department of Homeland Security.

U.S. Customs and Border Protection (CBP) is the unified border agency within the Department of Homeland Security (DHS). CBP combined the inspectional workforces and broad border authorities of U.S. Customs, U.S. Immigration, Animal and Plant Health Inspection Service and the entire U.S. Border Patrol.

CBP includes more than 41,000 employees to manage, control and protect the Nation's borders, at and between the official ports of entry. "U.S. Customs and Border Protection has accomplished a lot to secure our borders, but there is much more we are doing. We understand that as America's frontline, the security of a nation rests on our shoulders. We have learned the lessons of 9/11 and are working day and night to make America safer and more secure," stated Commissioner Robert C. Bonner.

CBP "Twin Goals" - Anti-Terrorism and Facilitating Legitimate Trade and Travel

"For the first time in our nation's history, one agency has the lone responsibility of protecting our borders. As the single, unified border agency, CBP's mission is vitally important to the protection of America and the American people. CBP's priority mission is preventing terrorists and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel," continued Commissioner Bonner.

CBP uses multiple strategies and employs the latest in technology to accomplish its dual goals. CBP's initiatives are designed to protect the homeland from acts of terrorism, and reduce the vulnerability to the threat of terrorists through a multi-level inspection process.

Better Targeting

U.S. Customs and Border Protection assess all passengers flying into the U.S. from abroad for terrorist risk. We are able to better identify people who may pose a risk through initiatives such as: the Advance Passenger Information System (APIS), United States Visitor and Immigrant Status Indication Technology (US-VISIT), and the Student and Exchange Visitor System (SEVIS). CBP regularly refuses entry to people who may pose a threat to the security of our country. This was not a focus prior to 9/11, but a shift in priorities and the formation of U.S. Customs and Border Protection has made this the top priority of the agency – keeping terrorists and terrorist weapons out of the country.

In addition, CBP uses advance information from the Automated Targeting System (ATS), Automated Export System (AES), and the Trade Act of 2002 Advance Electronic Information Regulations to identify cargo that may pose a threat. CBP's Office of Intelligence and the National Targeting Center (NTC) enhance these initiatives by synthesizing information to provide tactical targeting. Using risk management techniques they evaluate people and goods to identify a suspicious individual or container before it can reach our shores.

Photo Credit: Gerald L. Nino

The Automated Commercial Environment (ACE) has made electronic risk management far more effective. The ACE Secure Data Portal provides a single, centralized on-line access point to connect CBP and the trade community. CBP's modernization efforts enhance border security while optimizing the ever-increasing flow of legitimate trade.

CBP also screens high-risk imported food shipments in order to prevent bio-terrorism/agro-terrorism. For the first time, U.S. Food and Drug Administration (FDA) and CBP personnel are working side by side at the NTC to protect the U.S. food supply by taking action, implementing provisions of the Bioterrorism Act of 2002. CBP and FDA are able to react quickly to threats of bio-terrorist attacks on the U.S. food supply or to other food related emergencies.

Pushing Our "Zone of Security Outward" - Partnering With Other Countries

U.S. Customs and Border Protection has created smarter borders by extending our zone of security beyond our physical borders.

CBP has established working groups with our foreign counterparts to establish ties, improve security and facilitate the flow of legitimate trade and travel. Through the Container Security Initiative (CSI), CBP pushes our zone of security outward by working jointly with host nation counterparts to identify and screen containers that pose a risk at the foreign port of departure before they are loaded on board vessels bound for the U.S. CSI is now implemented in 20 of the largest ports in terms of container shipments to the U.S. and at total of 58 ports worldwide.

CBP has implemented joint initiatives with our bordering countries, Canada and Mexico: The Smart Border Declaration and associated 30-Point Action Plan with Canada and The Smart Border Accord with Mexico. The Secure Electronic Network for Travelers' Rapid Inspection (SENTRI) allows pre-screened, low-risk travelers from Mexico to be processed in an expeditious manner through dedicated lanes. Similarly, on our northern border with Canada, we are engaging in NEXUS to identify and facilitate low-risk travelers. Along both borders, CBP has implemented the Free and Secure Trade (FAST) program. The FAST program utilizes transponder technology and pre-arrival shipment information to process participating trucks as they arrive at the border, expediting trade while better securing our borders.

In addition, an agreement with Canada allows CBP to target, screen, and examine rail shipments headed to the U.S. This month, CBP is establishing CBP attachés in Mexico and Canada to coordinate border security issues. CBP Border Patrol agents, the Royal Canadian Mounted Police, and the Drug Enforcement Administration, as well as state and local law enforcement agencies from Canada and the U.S. have joined together to form fourteen Integrated Border Enforcement Teams (IBET). Covering our entire mutual border with Canada, these teams are used to target cross-border smuggling between Canada and the United States. The teams focus on criminal activity such as smuggling of drugs, humans, contraband and cross-border terrorist movements.

Pushing Our "Zone of Security Outward" - Partnering With the Private Sector

Processing the sheer volume of trade entering the U.S. each year requires help from the private sector. The Customs-Trade Partnership Against Terrorism (C-TPAT) is a joint government-business initiative designed to strengthen overall supply chain and border security while facilitating legitimate, compliant trade. To date, over 6,500 companies are partnering with CBP. C-TPAT is the largest, most successful government-private sector partnership to arise out of 9-11.

In addition, U.S. Customs and Border Protection is piloting the Advanced Trade Data Initiative. This program works with the trade community to obtain information on U.S. bound goods at the earliest possible point in the supply chain. Partnering with carriers, importers, shippers and terminal operators, we are gathering supply chain data and feeding it into our systems to validate container shipments during the supply process. This information increases CBP's existing ability to zero in on suspect movements and perform any necessary security inspections at the earliest point possible in the supply chain.

Inspection Technology and Equipment

Given the magnitude of CBP's responsibility the development and deployment of sophisticated detection technology is essential. Deployment of Non-Intrusive Inspection (NII) technology is increasing and viewed as "force multipliers" that enable CBP officers to screen or examine a larger portion of the stream of commercial traffic.

Photo Credit: Gerald L. Nino

CBP does not rely on any single technology or inspection process. Instead, officers and agents use various technologies in different combinations to substantially increase the likelihood that terrorist weapons including a nuclear or radiological weapon will be detected and interdicted.

Technologies deployed to our nation's land, sea, and airports of entry include large-scale x-ray and gamma-imaging systems. CBP has deployed radiation detection technology including Personal Radiation Detectors (PRDs), radiation isotope identifiers, and radiation portal monitors. CBP uses trained explosive and chemical detector dogs. CBP's Laboratories and Scientific Services Fast Response Team reacts to calls on suspicious containers. The Laboratories and Scientific Services also operates a 24 hours, 7 days a week, 365 days a year hotline at its Chemical, Biological, Radiation, and Nuclear Technical Data Assessment and Teleforensic Center.

Keeping Weapons and Money from Falling into Terrorist Hands – Outbound Inspections

U.S. Customs and Border Protection has the authority to search outbound, as well as in bound shipments, and uses targeting to carry out its mission in this area. Targeting of outbound shipments and people is a multi-dimensional effort that is enhanced by inter-agency cooperation. CBP in conjunction with the Department of State and the Bureau of the Census has put in place regulations that require submission of electronic export information on U.S. Munitions List and for technology for the Commerce Control List. This information flows via the Automated Export System (AES). CBP is also working with the Departments of State and Defense to improve procedures on exported shipments of foreign military sales commodities. CBP also works with Immigration and Customs Enforcement (ICE) to seize outbound currency, particularly cash and monetary instruments going to the Middle East.

Protecting the Miles of Open Border Between Official Ports of Entry

U.S. Customs and Border Protection's Border Patrol agents are better securing areas between the ports of entry by implementing a comprehensive border enforcement strategy, expanding, integrating, and coordinating the use of technology and communications through:

- Integrated Surveillance Intelligence System (ISIS) is a system that uses remotely monitored night-day camera and sensing systems to better detect, monitor, and respond to illegal crossings.

- Unmanned Aerial Vehicles (UAVs) are equipped with sophisticated on-board sensors. UAVs provide long-range surveillance and are useful for monitoring remote land border areas where patrols cannot easily travel and infrastructure is difficult or impossible to build.

- Remote Video Surveillance Systems (RVSS) provide coverage 24 hours a day, 7 days a week to detect illegal crossings on both our northern and southern borders.

- Geographic Information System (GIS) - a CBP Border Patrol southwest border initiative to track illegal migration patterns.

- "U.S. Customs and Border Protection can point to a myriad of accomplishments since 9/11 to better secure our Nation's borders. They are astonishing in scope and the speed with which we have implemented them. Our borders are more secure than they were on 9/11 -- keeping terrorists and their weapons out of our country is the most vital mission of any law enforcement agency – a mission we must succeed at," stated Commissioner Bonner.

Note: This article was originally published on 14 May 2008 on the U.S. Department of Homeland Security Web site, <CBP.gov>.

Securing the United States-Mexico Border: An On-Going Dilemma

Karina J. Ordóñez

Reprinted with permission from *Homeland Security Affairs.*

Introduction

For decades, the United States federal government has developed and implemented border security strategies to counter illegal cross-border activity. While some strategies have alleviated the influx of illegal immigration to certain geographic areas, increased border controls in these locations have made other, less controlled areas of the border more vulnerable. Rising crime rates, discarded debris, increased apprehension rates, and growing public scrutiny in these less secure areas provide clear evidence that border security is at once a social, an economic, and a national security issue.

Prior to 9/11, the United States Border Patrol (USBP) had established security efforts along the international border. Since then, however, the constant flow of unauthorized migrants and "the increasing mobility and destructive potential of modern terrorism has required the United States to rethink and rearrange fundamentally its systems for border… security."[1] Yet, despite the border security efforts of the Bush Administration and the United States Department of Homeland Security (DHS), the problem persists and continues to worsen, particularly along the Arizona-Sonora border (ASB). There is a critical need to rethink border security systems, particularly along the Southwest border, that leads observers to ponder: who is primarily responsible for securing our borders? What is the USBP doing to secure the border given the additional threat of terrorism? [2]

Defining Borders

In order to articulate functional definitions, the "border" refers to the 2,000 mile geo-political divide between the United States and Mexico. However, for purposes of this paper, the "border" is specifically the international border between the State of Arizona, United States and the State of Sonora, Mexico. The 377-mile Arizona-Sonora Border (ASB) is a portion of one of the world's busiest international boundaries and, as such, an overwhelming number of cross-border illegal and legal activities occur there daily.[3] Although there is a geo-political border, a full understanding of the complexities and dynamics of the ASB requires recognition and analysis of the communities on both sides of the border. The economic dependency, and the environmental and cultural ties between these border communities, adds a multifaceted dynamic and dimension to understanding the ASB. This cultural, social, and economic region has received recognition from governments and the public; therefore, to encompass these intrinsic interdependencies, the term "border region" was officially recognized in 1983 in the La Paz Agreement. The border region includes 100 kilometers (67 miles) north and south of the geopolitical divide between the United States and Mexico.[4] The border region has a population of approximately three million people, and it continues to grow exponentially as compared to the national average of both the United States and Mexico.[5] This includes all of the cities, town, communities, tribes, and counties within this area, which share common challenges.

9/11 brought a new dimension to the problem of illegal immigration with potential terrorists seeking to enter the country, thereby elevating border security to a national priority. The United States government responded to 9/11 with the creation of DHS, a department tasked with "preventing terrorist attacks within the United States, reducing American's vulnerability

to terrorism and minimizing the damage and recovery from attacks that do occur." [6] DHS was created under the Homeland Security Act of 2002 and merged twenty-two agencies into one department and ostensibly one mission. One of the newly created directorates was Border and Transportation Security, which abolished the Immigration and Naturalization Services (INS) and divided its functions among Citizenship and Immigrant Services (CIS), Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG), and Customs and Border Protection (CBP). While these units continue to exist within DHS, the directorate of Border and Transportation Security was recently disbanded by Secretary Chertoff, in July 2005. Now, CIS processes legal immigration services and enforces illegal immigration along with the USCG, ICE, and CBP. The duties of illegal immigration enforcement are further divided between ICE and CBP: ICE enforces immigration law within the interior of the United States and CBP, USBP enforces and protects the United States border. The goal in integrating customs inspectors, immigration inspectors, and agricultural inspectors under CBP was to provide one face at the border and one comprehensive strategy with a unity of force. However, USBP – although a unit of CBP – remains distinct, with its own mission and force.

By law and according to the *National Border Patrol Strategy,* CBP is the authoritative law enforcement agency charged to protect the nation's borders and ensure that the United States is not penetrated by terrorists, unauthorized migrants, human smugglers, human traffickers, drug smugglers, or contraband.[7] Under the auspices of a new directorate, the priority mission of the USBP is homeland security, defined as "nothing less than preventing terrorists and terrorist weapons – including potential weapons of mass destruction – from entering the United States." [8] The priority mission functionally establishes and maintains operational control of the United States border between the ports of entry (POE). On the other hand, it is CBP's mission to control the United States border as a whole. The aftermath of 9/11 caused policy makers to expand the traditional mission to include preventing terrorists and terrorist weapons from entering the United States, in addition to "interdicting illegal aliens and drugs and those who attempt to smuggle them across our borders." [9] The USBP's area of operation and responsibility is between land and sea POE, which extends across 7,000 miles of border with Canada and Mexico and 12,000 miles of coastal borders.

Border Strategy, 1994-2004

While the USBP patrols both the northern and southern borders, 90 percent of USBP resources are deployed along the United States-Mexico Border (USMB) because it is considered the focal point for illegal immigration with ninety-seven percent of all illegal alien apprehensions.[10] The four border states along the USMB are divided into nine USBP Sectors: San Diego and El Centro, California; Yuma and Tucson, Arizona; El Paso (New Mexico and two counties in Texas); Marfa, Del Rio, Laredo and McAllen, Texas. While these four states share a geopolitical and geo-physical border with Mexico, they do not share the same topography, climate, or challenges. Accordingly, the USBP faces the challenge of developing different operational tactics and techniques for each sector.

Tucson Sector represents forty-three percent of the total annual Southwest USBP's apprehensions.[11] This percentage indicates that most of the illegal cross-border activity occurs within 262 miles of the total 2,000 miles of international border with Mexico.[12] Table 1 indicates that in the past decade the Tucson Sector has become the most active in terms of illegal cross-border activity, with a significant increase in total apprehensions along the Southwest border: from eight percent in 1993 to forty-three percent in 2004.

U.S. Border Patrol
Apprehension Statistics 1993 - 2004
Data Presented in Actual Numbers and
as a Percentage of Total Southwest Apprehensions

Border Patrol Sector	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Total Southwest	1,212,886	979,101	1,271,390	1,507,020	1,368,707	1,516,680	1,537,000	1,643,679	1,235,717	929,809	905,065	1,138,282
San Diego, CA	531,689	450,152	524,231	483,815	283,889	248,092	182,267	151,681	110,075	100,681	111,515	138,608
El Centro, CA	30,058	27,654	37,317	66,873	146,210	226,695	225,279	238,126	172,852	108,273	92,099	74,467
Yuma, AZ	23,548	21,211	20,894	28,310	30,177	76,195	93,388	108,747	78,385	42,654	56,638	98,060
Tucson, AZ	92,639	139,473	227,529	305,348	272,397	387,406	470,449	616,346	449,675	333,648	347,263	490,771
El Paso, TX	285,781	79,688	110,971	145,929	124,376	125,035	110,857	115,696	112,857	94,154	88,816	104,399
Marfa, TX	15,486	13,494	11,552	13,214	12,692	14,509	14,952	13,689	12,087	11,392	10,319	10,530
Del Rio, TX	42,289	50,036	76,490	121,137	113,280	131,058	156,653	157,178	104,875	66,985	50,145	53,794
Laredo, TX	82,348	73,142	93,305	131,841	141,893	103,433	114,004	108,973	87,068	82,095	70,521	74,706
McAllen, TX	109,048	124,251	169,101	210,553	243,793	204,257	169,151	133,243	107,843	89,927	77,749	92,947

Border Patrol Sector	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
San Diego, CA	44%	46%	41%	32%	21%	16%	12%	9%	9%	11%	12%	12%
El Centro, CA	2%	3%	3%	4%	11%	15%	15%	14%	14%	12%	10%	7%
Yuma, AZ	2%	2%	2%	2%	2%	5%	6%	7%	6%	5%	6%	9%
Tucson, AZ	8%	14%	18%	20%	20%	26%	31%	37%	36%	36%	38%	43%
El Paso, TX	24%	8%	9%	10%	9%	8%	7%	7%	9%	10%	10%	9%
Marfa, TX	1%	1%	1%	1%	1%	1%	1%	1%	1%	1%	1%	1%
Del Rio, TX	3%	5%	6%	8%	8%	9%	10%	10%	8%	7%	6%	5%
Laredo, TX	7%	7%	7%	9%	10%	7%	7%	7%	7%	9%	8%	7%
McAllen, TX	9%	13%	13%	14%	18%	13%	11%	8%	9%	10%	9%	8%

Table 1. United States Border Patrol Apprehension Statistics 1993 – 2004. From: United States Border Patrol, "Apprehension Statistics 1993 -2004: Data Presented in Actual Numbers and as a Percentage of Total Southwest Apprehensions," http://www.lawg.org/docs/apprehension%20stats.pdf.

According to the INS, this phenomenon is a tactical dimension of the INS' *National Strategic Plan,* which accounts for various ways to control the influx of illegal immigration in the concentrated border areas of San Diego and El Paso. In 1994, the INS focused enforcement efforts in San Diego and El Paso; the goal was to shift migrants outside of the urban area, to more open areas, a strategic and tactical intention of INS. The intention was not to shift migrants into different jurisdictions; instead it was to continue shifting the migrants and break up criminal networks by gaining control in the less secure areas over time. As indicated by the USBP Chief David Aguilar:

> Historically, major CBP Border Patrol initiatives, such as Operation Hold the Line, Operation Gatekeeper, and Operation Rio Grande in our El Paso, San Diego, and McAllen Sectors, respectively, have had great border enforcement impact on illegal migration patterns along the southwest border, proving that a measure of control is possible. Together, these border security operations have laid the foundation for newer strategies and enforcement objectives and an ambitious goal to gain control of our Nation's borders, particularly our border with Mexico.[13]

Border security experts argue that the border security strategy is at a stage where the migration flow is concentrated in Arizona. However, this concentration can be due to changes in leadership, administrations and a non-continuous flow of resources to these less secure areas, leaving the

Tucson Sector as the primary gateway for illegal cross-border activity along the USMB. The various border operations mentioned in Chief Aguilar's testimony are part of the first phases of the overall national border security strategy developed in the early 1990s. DHS is developing and implementing new strategies – such as the Arizona Border Control Initiative – to continue the border security strategy's second phase in minimizing the vulnerabilities along the international border.

A review of USBP strategy from 1993 to 2004 will help illuminate how these particular USBP strategies led to the current challenges faced by the Arizona Tucson Sector. The build-up of border enforcement along the USMB first started in the early 1990s under the Clinton Administration, in response to public concern about illegal immigration from Mexico and its effect on public services and employment in the United States.[14] Experts called for a strategy that would simultaneously increase tighter enforcement of United States immigration laws while the North American Free Trade Agreement (NAFTA) spurred Mexican economic growth. Together, these experts asserted, both would help reduce the flow of illegal immigration from Mexico to the United States. Consequently, INS designed several border security strategies to prevent illegal cross-border activity. These strategies derived from a mixture of community policing theory and a low-intensity warfare concept. In addition, the challenges along the border were concentrated, and the need to protect the international border from illegal entry caused border security experts to research and implement new theories. Border security strategies focused on deterrence by deploying large numbers of border patrol agents, increasing the hours of actual border patrolling, and enhancing border security technology. These resources were deployed to strategically designated areas of the Southwest border with the greatest number of crime and disorder. During this period, the San Diego and El Paso sectors represented the gateways used by 70-80 percent of the unauthorized migrants entering the United States.[15] The strategy made sense and the demand for federal response resulted in the implementation of this strategy with the greatest border security funding appropriation in United States history.

Rather than spread the resources across the entire USMB, the INS "concentrated border enforcement strategies" were implemented in four specific segments of the international border: Operation Hold-the-Line in El Paso, Texas in 1993, Operation Gatekeeper in San Diego in 1994, Operation Rio Grande for South Texas in 1997, and Operation Safeguard in central Arizona in 1995.[16] These strategies were developed with the intention of increasing the USBP's probability of apprehension to a level that would deter potential migrants from crossing into El Paso or San Diego. Eventually, the intent was for border crossers to "spread the word" on the difficulty of entering the United States (without being apprehended) to potential migrants and deter them from leaving their hometowns in Mexico and other countries.

Operation Safeguard began operations in 1999 in Nogales, Arizona. It was not until 1999 that USBP in Arizona began to participate in the concentrated border enforcement strategy. Some experts argue that this was because Arizona contains extensive natural hazards, which were perceived as a deterrent to migrants attempting a clandestine entry into the United States. Former INS Commissioner Doris Meissner believed no one would risk their lives to illegally cross the border in areas of formidable mountains and extreme desert temperatures.[17] Essentially, "Mother Nature" would take care of USBP's responsibility. However, experts were incorrect in this assumption, as seen by the significant loss of life by many migrants attempting to cross in these geographically desolate areas.[18]

A Strategy for the Next Decade

Our nation is still facing a steady increase in the number of illegal immigrants residing in our communities along with an increase in the number of deaths in the desert; both demonstrate that the current border enforcement system is flawed.[19] Roughly ten years after the implementation of the INS *Strategic Plan*, border security remains a critical national mission. Throughout this period, the United States has increased funding for immigration control and border security initiatives. These increases have not translated into a more secure border and are still deemed inadequate to meet the post-9/11 mission. According to the Search for International Terrorist Entities (SITE) Institute, the border enforcement policy was unsuccessful because "despite extensive surveillance, the border remains porous because of the stretches of desert it crosses and Mexico's established smuggling networks."[20] This premise was a component of the INS National Strategic Plan, yet the border remains insecure.

While these border security efforts had a significant impact in the San Diego and El Paso Sector, less secure sectors are suffering from the incomplete multi-phase implementation of the National Border Strategy. The ASB current border insecurity situation is due to the incomplete implementation of the National Border Strategy Phase II; insufficient resources continue to be deployed within the Tucson Sector.

Two main factors contribute to the ever-increasing demands placed upon border security resources along the USMB. First, the pressure of enhanced law enforcement strategies in certain sectors has resulted in a shift of migrants from more secure urban areas to those rural communities that are less protected and populated.[21] For example, as crime rates dropped in San Diego and El Paso, due to more concentrated border security efforts, the Tucson Sector experienced an increase in illegal activity supplemented by violent crimes of auto-theft, extortion, rape, and homicide. Moreover, on a statewide basis, both Arizona and Sonora are currently facing higher crime rates. Arizona ranks first in auto-theft and third in homicide in the United States, while Sonora ranks third in homicide in Mexico.[22]

Second, Mexico is experiencing an influx of Islamic migrants.[23] Conceivably, as the United States government increases security measures and tightens immigration law, potential terrorists may seek the assistance of human smugglers to infiltrate the porous international border. If this proves to be the case, then the policymakers should ask the same question that Arizona Senator Kyl posed on August 27, 2004: "Why wouldn't those seeking to attack America be tempted to join the hundreds of thousands already illegally entering from Mexico?"[24] In fact, intelligence collected from domestic and international law enforcement communities indicates that terrorists are seeking other means to enter the United States.[25] As terrorist organizations continue to network in Mexico and exploit sophisticated organized smuggling rings, the USBP could seemingly be faced with a new paradigm: human smugglers, colloquially known as Coyotes, as potential terrorist partners.

As noted, in the early 1990s the USBP launched a concentrated border security strategy in the El Paso and San Diego Sectors causing migrants and smugglers to move their operations to less secure sectors along the USMB. The United States General Accounting Office report suggests that these strategies showed positive results for both sectors. However, the remaining seven

sectors along the Southwest border saw an increase in illegal cross-border activity, particularly the Tucson Sector. In 1993, the San Diego Sector represented 43.6 percent of the Southwest border apprehensions, and the El Paso Sector represented 23.6 percent.[26] Yet, as the USBP claimed victory in the San Diego and El Paso Sectors with a reduction in apprehensions by 6 percent and 72 percent, respectively, the Tucson Sector experienced an increase of 50 percent.[27] This increase is a clear indication of the *balloon effect* along the USMB: the displacement of illegal cross-border activity to another, less secure, sector of the international border. This phenomenon was an intended consequence of the *National Strategic Plan* and demonstrated that the border control efforts in the San Diego and El Paso Sectors were working. However, the migrant flow shift was not intended to stop in the USBP Tucson Sector; instead, the intent was to continuously shift migrants from one sector to another causing disruption of organized smuggling rings. This strategy derives from the theory of hot spots and the practice of community-oriented policing.

Place-oriented crime prevention strategies, a component of community policing, are commonly used by law enforcement agencies throughout the United States. The theory behind place-oriented crime prevention suggests that crime occurs in clusters, or "hot spots," and is not evenly distributed throughout the United States. As defined by the United States Department of Justice, Office of Justice Programs:

> A hot spot is an area that has a greater than average number of criminal or disorder events, or an area where people have a higher than average risk of victimization. This suggests the existence of cool spots – places or areas with less than average amount of crime or disorder.[28]

This phenomenon is used by individuals every day, evidenced by the places people tend to avoid given their probability of victimization. This suggests that crime is not evenly distributed. One can deduce that the *National Strategic Plan* drew from this theory; this is evident because resources were focused in the urban areas. The USBP continues to implement strategies that are complementary to community policing. Experts suggest that this "hot spots" phenomenon is supported by three complementary theories: environmental criminology, routine activities, and rational choice. Environmental criminology theory explores and analyzes the environment in which a criminal act is conducted. The analysis takes into consideration the criminal interaction with targets, the opportunities across space and time, and the characteristics of the area, such as safe havens. Routine activities theory is based on the notion that in the absence of a capable guardian, crime occurs when the bandit comes into close proximity of a potential target. Rational choice theory is based on the belief that bandits are capable of making their own decisions and opt to commit crime in order to benefit.

Another interesting analysis that is drawn from community-policing is that as law enforcement pressure is applied in "hot spots," crimes begin to emerge in "cool spots." Experts claim "focused police interventions, such as directed patrols, proactive arrests, and problem solving, can produce significant crime prevention gains at high-crime 'hot spots.' " [29] In a nutshell, "hot spot" policing suggests that if the environment is manipulated (i.e., increased patrols, arrests, etc.), then victims and offenders have fewer interactions and bandits have fewer opportunities to commit crimes, which ultimately results in a decrease in the crime rate. In addition, once a "hot spot" is controlled and crime has decreased, bandits will move to a less patrolled area to continue their criminal activities. These criminal migrations are occurring at the Southwest border. Apprehension statistics are a clear indication that illegal border crossers (IBC) have migrated to areas less patrolled by USBP, such as the Tucson Sector.

The USBP has focused its resources in the urban areas along the international border for a variety of reasons, such as preventing bandits from interacting with border community residents and restricting bandits from access to safe havens or camouflaging into the community. In addition, the *balloon effect* experienced in the Tucson Sector parallels the concept of "hot spots" in urban areas. Once the community policing addresses a "hot spot" crime area, the crime moves into a less policed area. Similarly, when the USBP focuses enforcement efforts along the USMB, migrants and bandits move into less secured sectors. This shift was the intention of the USBP's concentrated border security strategy. Therefore, USBP was not surprised to see bandits and smugglers moving towards the Tucson Sector.

Why, then, isn't the USBP Tucson Sector prepared to handle the influx of migrants? The answer could be a combination of issues – politics, resources, or the simple notion that geographical constraints would be a sufficient deterrent for migrants entering the United States. The United States government must continue to develop and implement timely border security strategies that take into consideration the movement of illegal activities along the border in order to successfully secure the USMB, as described above. However, the post-9/11 need to protect the United States from another terrorist attack requires intelligence analysts to observe for potential emerging terrorist threats along the international border and then quickly address these threats with stealth and innovation.

One Solution: The ASB Model

While the efforts of Congress and the USBP continue, the illegal immigration problem persists and becomes increasingly divisive in communities nationwide. The current deployment and employment of resources must be revisited to increase efficiency and alleviate the challenges along the USMB. The application of force along the border, without the proper use of intelligence to modify the use of force in a timely and adequate manner along the USMB, could potentially accelerate the "balloon effect." The use of the Arizona-Sonora Border (ASB) model or a similar border model would allow strategists to minimize the geographical displacement effects prior to applying force along the USMB.

The ASB model is an analytic model that incorporates factors relevant to the problem of illegal cross-border activity in the USBP Tucson Sector. While a model can never fully reflect the true complexity of illegal cross-border activity factors, illegal cross-border activity has some structural features that lend themselves to analytical modeling. In other words, illegal cross-border activity is not a random event; it exhibits organized and structured occurrences and can be modeled. The ASB model is a "plug and play" model that can assist in forecasting what may occur along the border within a five day window, given certain IBCs' distribution and USBP resource deployment. The model does not project actual numbers of IBCs, but rather the success rate of the USBP as a function of the infiltration and migration patterns, and the resources mix. Given a certain distribution of IBCs, and different migration rates, the question is: how should USBP Border Security resources be deployed to be most effective? Specifically, the model examines the effect of apprehension rates (which depend on the resources mix) on the number of IBCs that successfully evade the USBP. Given the functional relation, one can calculate the desired deployment of resources in order to optimize effectiveness.

The purpose of the ASB model is to assist policymakers and operational planners to address the problem of illegal cross-border activity with a logical and systematic approach. The mathematical model can help organize, articulate, and analyze the essential problems in the USBP Tucson Sector. The ASB model provides insight into the complex interdependencies that exist in establishing and maintaining control of the international border with Mexico. It captures

the interactions among the location and intensity of cross-border activities, apprehension rates, and migration rates. This model is an attempt to offer a mathematical solution to the problem of optimal deployment of border security resources in the USBP Tucson Sector along the ASB. The appropriate employment and deployment of border security resources can minimize illegal cross-border activity and reduce the border's vulnerabilities.

Conclusion

The ASB model examines illegal cross-border activity situations in the USBP Tucson Sector, or any part of it, and forecasts the effectiveness of USBP border security resources deployment. Although this model is specific to the USBP Tucson Sector, it can be implemented anywhere along the Southwest Border with minor modifications. The ASB model demonstrates that by increasing border security enforcement efforts, it may augment humanitarian concerns along the USMB. As migrants move away from high enforcement areas to low enforcement areas, in other words, they move away from areas where the border security enforcement is more effective, and are thus exposed to greater natural hazards. Therefore, as operational planners and policy makers develop new strategies, these humanitarian concerns and consequences need to be taken into consideration in order to reduce deaths in the desert and improve bi-national relations with Mexico.

Karina J. Ordóñez is the strategic policy coordinator for the Arizona Department of Homeland Security. In this capacity, she is the primary advisor to the deputy director in matters pertaining to national policy and serves as the state agency liaison focusing on public health, agro-terrorism, bioterrorism, and disaster preparedness. Special projects in her portfolio include developing the State Homeland Security Strategy and the State Infrastructure Protection Plan. She is a graduate of the Naval Postgraduate School's Center for Homeland Defense and Security.

End notes

1. Office of Homeland Security, *National Strategy for Homeland Security* (Washington DC: Government Printing Office, July 2002), 21.

2. This paper is drawn from Karina J. Ordóñez, Modeling the U.S. Border Patrol Tucson Sector for the Deployment and Operations of Border Security Forces, M.A. thesis, Naval Postgraduate School, 2006.

3. United States Border Patrol, "Apprehension Statistics 1993 -2004: Data Presented in Actual Numbers and as a Percentage of Total Southwest Apprehensions" (2005), http://www.lawg.org/docs/apprehension%20stats.pdf.

4. La Paz Agreement defined the border region as 100 km north and 100 km south of the United States-Mexico International border. See "La Paz Agreement," (August 14, 1983). Text of the La Paz Agreement, including Annex I-V is available at http://yosemite.epa.gov/oia/MexUSA.nsf/La+Paz+Agreement+-+Web?OpenView&ExpandView.

5. United States Bureau of the Census, *Annual Estimates of the Population for Counties of Arizona: April 1, 2000 to July 1, 2004,* COEST2004-01-04 (Washington DC: Population Division, United States Census Bureau, 2005), and El Instituto Nacional de Estadísticas, Geográfica e Informática (the Mexican Bureau of Statistics, Geography and Computer Science), *Estadísticas de Población por Estado (Population Statistics by State),* 2000.

6. Office of Homeland Security, *National Strategy for Homeland Security* (Washington DC: Government Printing Office, July 2002), 2.

7. The Labor Appropriation Act of 1924 established the United States Border Patrol in response to rising illegal entries particularly along land borders.

8. Robert C. Bonner, *National Border Patrol Strategy: Message from the Commissioner* (Washington DC: United States Customs and Border Protection, Office of Border Patrol and the Office of Policy and Planning, September 2004).

9. Ibid.

10. Lisa Seghetti, et al., "Border Security and the Southwest Border: Background, Legislation, and Issues," #RL33106 (Washington, DC: Congressional Research Service, September 28, 2005): 21.

11. United States Border Patrol. "Apprehension Statistics 1993 -2004."

12. The illegal cross-border activity accounted for is the activity that is observed and interdicted.

13. David Aguilar, United States Border Patrol Chief, testimony before the House Committee on Appropriations and Subcommittee on Homeland Security, July 12, 2005. http://usinfo.state.gov/gi/Archive/2005/Jul/14-680142.html

14. Wayne Cornelius, "Controlling 'Unwanted' Immigration: Lessons from the United States, 1993 – 2004" (San Diego, CA: University of California Center for Comparative Immigration Studies, December 2004), 2.

15. Ibid., 6.

16. The majority of resources for Operation Safeguard did not arrive until 1999.

17. Cornelius, "Controlling 'Unwanted' Immigration," 6.

18. Bill Vann, "Five Years of Operation Gatekeeper: U.S. Border Crackdown Deaths Souring," *International Committee of the Fourth International (ICFI),* June 25, 1999, http://www.wsws.org/articles/1999/jun1999/ins-j25.shtml.

19. Jeffrey Passel, "Unauthorized Migrants: Numbers and Characteristics," *Pew Hispanic Center,* June 14, 2005. http://pewhispanic.org/reports/report.php?ReportID=46

20. Richard B. Schmitt, et al., "U.S. Fears Terrorism Via Mexico's Time-Tested Smuggling Routes," *SITE Institute*, September 15, 2004, http://www.siteinstitute.org/bin/articles.cgi?ID=news18904&Category=news&Subcategory=0.

21. This is one theory with regards to the displacement of migrants along the USMB. An alternative theory is the economic growth rates experienced in Phoenix and Las Vegas. These two cities are experiencing a fast growth rate followed by an increase in construction and employment. This boom in jobs in Nevada and Arizona causes the illegal migrant flow to switch to follow the employment opportunities.

22. Arizona Criminal Justice Commission, *Arizona Crime Trends: A System Review,* Statistical Analysis Center Publication, July 22, 2005, http://azcjc.gov/pubs/home/Crime_Trends_2005.pdf. Consejo de Seguridad Publica, "Programa de Mediano Plazo 2004 -2009: Seguridad Publica," http://www.sonora.gob.mx/biblioteca/documentos/pmp/seguridad.pdf.

23. A few days after 9/11, Mexican authorities detained 126 undocumented Iraqis in Mexico City. Since all Middle Easterners are supposed to have a VISA to enter the country, this presented a new problem for Mexican authorities: how did these people enter the country? Centro de Investigaciones Económicas y Política de Acción Comunitaria, "Guerra Mundial: Consecuencias Para México," November 21, 2001, http://www.ciepac.org/bulletins/200-300/bolec267.htm

24. Senator Jon Kyl, "Arizona: a 'Terrorist Corridor?'" Guest Opinion, *The Arizona Conservative,* August 27, 2004, http://www.azconservative.org/Kyl_TerrorismCorridor.htm.

25. Admiral James Loy, United States Department of Homeland Security deputy secretary, testimony before the Senate Select Committee on Intelligence, February 16, 2005. http://www.dhs.gov/xnews/testimony/testimony_0030.shtm

26. United States General Accounting Office, *Border Control: Revised Strategy is Showing Positive Results,* Report to the Chairman, Subcommittee on Information, Justice, Transportation and Agriculture, Committee on Government Operations, House of Representatives, Washington DC, December 1994: 11.

27. Ibid.

28. Office of Justice Programs, *Mapping Crime: Understanding Hot Spots* (Washington DC: United States Department of Justice, August 2005), http://www.ojp.usdoj.gov/nij.

29. Ibid.

Note: This article was originally published in the April 2008 edition of *Homeland Security Affairs.*

The El Paso Intelligence Center: Beyond the Border

Anthony P. Placido, Chief of Intelligence, U.S. Drug Enforcement Administration

Reprinted with permission from *Police Chief Magazine.*

On a sleety, cold afternoon in mid-January, Mississippi Highway Patrol troopers stopped a freight truck on Interstate 10 in Jackson County for not displaying a U.S. Department of Transportation number. While the troopers were inspecting the vehicle, they became suspicious of the driver's story that he was returning from New Jersey, where his cargo of rotting oranges—still in the trailer—was rejected. Officer Ricky Lott made a quick call to the El Paso Intelligence Center (EPIC). Five minutes later, EPIC alerted Officer Lott that the driver was a known drug smuggler with prior arrests in Florida on charges of money laundering and smuggling 8,600 pounds of marijuana across the border a decade earlier.

Based on the information EPIC provided, Officer Lott immediately had a better understanding of his situation that afternoon. He and his colleagues obtained consent to search the truck. Hidden among the rotting oranges they found $1.2 million in U.S. currency. The money was seized and the suspect was arrested; as a result, that much less drug money was available to line the pockets of foreign drug cartels. The cost of getting the additional information needed to stop the suspect: one toll-free telephone call that lasted five minutes.

Half a world away from Mississippi, EPIC research was vital to one of England's most critically important investigations. Shortly after the London subway bombings in July 2005, European Command contacted EPIC and requested that researchers there run the names of four of the bombing suspects through the EPIC databases. EPIC's analysis showed that one suspect had visited the United States, entering with a British passport, and located his address in Cleveland, Ohio, as well as the address of the apartment complex in which his mother frequently stayed. At the apartment, investigators learned that another individual residing there had an international terrorist connection and was responsible for funding terrorist activities. EPIC research also identified 16 other people in the terrorist cell within the United States.

These investigations demonstrate what EPIC does best: collect, analyze, and share with law enforcement organizations sensitive information that turns suspicion into probable cause, contraband into evidence, and suspects into criminal defendants.

A Jewel in the Desert

Situated in the west Texas desert, a stone's throw from the shallow Rio Grande and within view of Ciudad Juarez, Mexico—home to one of Mexico's most brutal drug cartels—sits EPIC. Its proximity to the Juarez cartel is an irony not lost on EPIC personnel, who provide real-time intelligence that helps law enforcement target the U.S. distribution networks of the Juarez and other drug cartels at every turn. Except for the palm trees out front, EPIC looks like any other government building. But a look inside reveals the extraordinary nerve center of the fight against transnational crime as well as a high-tech web of law enforcement databases. Led by the Drug Enforcement Administration (DEA), EPIC is staffed by 15 federal agencies from the Departments of Homeland Security, Justice, Transportation, and Defense, as well as state, county, and soon municipal law enforcement organizations.

Hundreds of special agents, intelligence analysts, computer and communications specialists, translators, technology experts, and support staff sift through complex, seemingly unrelated pieces of information. Fashioning useful intelligence by tying together the available data, the whole staff works to build probable cause for the apprehensions, asset seizures, indictments, and arrests of entire criminal organizations and their networks, thereby demolishing them. No other agency in the United States provides this kind of real-time tactical support to the law enforcement community with such a wide range of simultaneous database queries.

Beyond the Southwestern Border

IACP president Joseph Carter held an IACP Executive Committee meeting at EPIC in December 2006 at the invitation of DEA administrator Karen P. Tandy. In April of this year, EPIC hosted members of the IACP's Narcotics and Dangerous Drug Committee. These visits gave IACP leadership the opportunity to observe the internal workings of EPIC and see firsthand the broad support that EPIC provides to law enforcement. As a result of its visit, the committee is considering a resolution making EPIC the site of a two-week rotation for IACP-sponsored law enforcement personnel.

Every police executive should know that EPIC is a tremendously valuable free resource for local officers. The benefits of working with EPIC have been relatively unknown until now, in part because officers thousands of miles from the southwestern U.S. border do not realize that EPIC's intelligence is not limited to the actual border area itself. Karen Tandy hopes to change the perception that EPIC is helpful only to law enforcement in border states: "While EPIC always has had a southwest border address and focus, it also has a long history of information sharing that extends into the heartland of America and provides support to police in all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, and Guam. This information sharing is vital to officer safety, interdiction efforts, and investigations everywhere—not just along the border."

Last year, EPIC handled more than 75,000 queries from federal, state, local, and tribal law enforcement officers in all 50 states. With the expanding need for timely and accurate information, particularly since the tragedy of the September 11 terrorist attacks, EPIC not only provides a resource that the entire community—and most especially state and municipal departments—can rely on, but also intends soon to improve access to its resources for a wider range of customers.

Figure 1. Systems and Databases Available for Query
National Seizure System (NSS)—EPIC
Treasury Enforcement Communications System II (TECS II)—U.S. Immigration and Customs Enforcement
Central Index System (CIS)—Bureau of Customs and Border Protection
Sentry—Federal Bureau of Prisons
Warrant Information Network (WIN)—U.S. Marshals Service
Narcotics and Dangerous Drugs Information System (NADDIS)—Drug Enforcement Administration
Aircraft Registration System—Federal Aviation Administration

Protection of Sensitive Information

Over the years, EPIC has quietly learned to strike the right balance between the desire to share information and the need to protect sensitive intelligence sources and methods. This balance is achieved by carefully managing dissemination of information through a tiered-access system, where prospective users are carefully screened so that they can receive information from closed investigations or from nonsensitive sources immediately. When users request information related to an ongoing sensitive investigation or source, they are notified that information is available and are provided with contact information for the relevant personnel. This pointer mechanism allows users to negotiate access to sensitive information on a case-specific basis while maintaining immediate access to a much larger set of less sensitive information.

EPIC has vast data holdings that include information from many federal, state, and local agencies (see figure 1). As the center has grown, it also has taken on the role of information hub for the High Intensity Drug Trafficking Area (HIDTA) investigative support centers as it continues to provide direct support to an ever-expanding list of participating agencies. Most of the information from this wide array of databases can be gathered instantly with a single query of EPIC's confederated databases.

Three Ways EPIC Can Help

The heart and soul of the 33-year-old center is EPIC Watch, a communications center that takes inquiries from law enforcement by phone, facsimile, or e-mail 24 hours a day, 365 days a year. EPIC has unique access to information concerning aircraft, vessels, and firearms. Subject matter experts are available through the Watch to answer questions; trace weapons; or place lookouts for suspect vehicles, vessels, or aircraft.

With a single call to EPIC, an officer who has pulled over a subject can determine if the individual has a record of being armed or dangerous; if the vehicle has recently crossed the border from Mexico; or if any of the individuals in the vehicle are currently or previously have been the subject of any investigations. In short, this single point of contact and the rapid access to the broadest possible array of information provides law enforcement officers with three principal benefits: enabling officers to make better-informed judgments, protecting their safety, and increasing their likelihood of success.

The first benefit EPIC can provide is to give state and local police officers the kind of information they need to make better decisions. For example, when one Ohio state highway patrolman stopped a vehicle for a traffic violation, the officer noticed that the car had a fraudulent temporary registration, making him suspicious of the driver and passenger. He called EPIC Watch and asked for a full records check. EPIC responded with the information that the passenger had numerous drug-related offenses dating back to 1995 and that the suspect was known to conceal contraband in certain locations. After having obtained consent to search the car, the trooper discovered 90 kilograms of cocaine hidden in false compartments.

In addition, EPIC's information can protect officers. Art Doty, director of EPIC, notes that the center's typical customer is "alone officer or deputy sheriff who has a suspicious vehicle pulled over on a lonely stretch of road in the middle of the night." Many times a search of EPIC's databases have alerted officers that the individual they have pulled over on a traffic stop is known to be armed and dangerous, a violent felon, or a fugitive from the law. Certainly it's the kind of information any officer wants to know—the kind of information that saves officers' lives.

Finally, intelligence obtained from EPIC can increase the likelihood of case success—and even increase the investigative impact of some cases. Consider the following example. Texas Department of Public Safety officers seized $785,000 from a freight truck in December 2005. Fingerprints on the seized money wrappers were identified as belonging to a fugitive who is a member of Los Zetas, the enforcement arm of the Gulf cartel. The DEA's Houston office asked EPIC to help identify the fugitive's assets. EPIC discovered 14 businesses, 22 real property assets, and 79 conveyances, with a total value of $3.3 million. So far, the DEA has seized two of the fugitive's houses, with seizures on the other assets pending.

Free and Easy

The best part about EPIC may be its cost: nothing. It's completely free to join and easy to do so. Figure 2 provides information on how to apply for participation. After receiving an application, EPIC personnel process it, vet the applying department's officers, and grant access in a short time—anywhere from a day to a couple of weeks, depending on the size of the department. Once officers have access, it's as easy as dialing, toll-free, 1-888-USE-EPIC.

The DEA is making access to EPIC even easier and better than ever. The center's new open connectivity project is about to make EPIC's vast pool of information more readily available to federal, state, and local police officials via an inexpensive, secure Internet connection. The first phase of this effort, already under way, allows participating agencies to both provide and

retrieve information from the National Seizure System and the Clandestine Laboratory Seizure System. These systems provide a comprehensive picture (using geospatial information system technology) of drug, currency, weapon, and laboratory seizures—literally mapping out such seizures to assist law enforcement in tactical and strategic planning efforts. Ultimately, this secure Web portal will allow authorized users to gain access via the Internet to the same sensitive law enforcement and investigative data that are currently available by contacting EPIC Watch.

Cop-to-Cop Discussions

In addition to housing data from participating agencies, the center has its own unique internal database that contains a 33-year history of the law enforcement agencies and officers who have made inquiries about particular suspects, vehicles, vessels, or aircraft. The center keeps this critical information because the concealed compartment that was empty during one traffic stop may not be on the next encounter. EPIC's internal database and the use of pointer information overcome one of the major obstacles to information sharing: promoting "cop-to-cop" discussions and facilitating the sharing of critical information that was never put in writing and does not appear in any automated database.

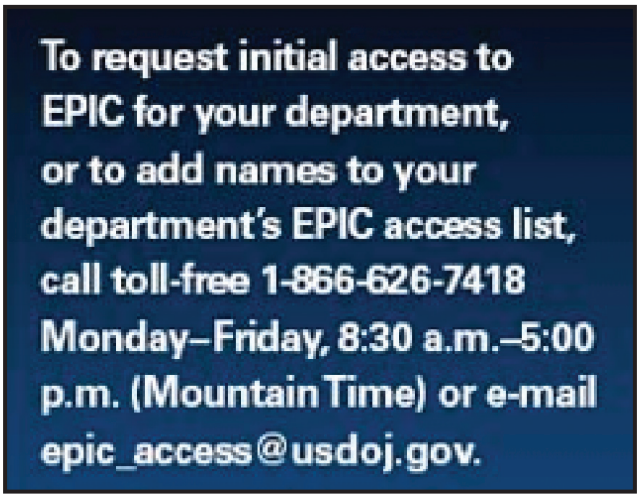
Research and Analysis: There for the Asking

EPIC augments its critical Watch function by performing analyses of drug movement events, trends, and patterns, as well as research and analysis of criminal organizations. The resulting bulletins and reports are routinely sent to participating state and local departments, alerting them to the latest drug trafficking information. For example, in December 2006, EPIC distributed a bulletin that included an analysis of 261 drug seizure incidents along highways in Tennessee, Alabama, Georgia, North Carolina, and South Carolina that showed drug smuggling patterns in the last year.

EPIC reports can also notify recipients of dangers that officers could encounter, such as new developments in hidden weapons or explosives.

Training

Since the implementation of the Operation Pipeline drug interdiction program, EPIC has hosted Operation Pipeline schools throughout the United States. Pipeline training is one of the most practical training sessions available in law enforcement. Instructors for these three-day schools include fellow officers with years of experience in highway interdiction and local prosecutors and assistant U.S. attorneys who instruct officers on the laws and policies governing highway stops. All Pipeline schools include general core instruction on such topics as development of probable cause; asset forfeiture and asset sharing; concealment detection and hidden compartments; violator indicators; interview techniques; record checks and information sharing; and intelligence exchange among federal, state, and local agencies, as well as a practical exercise at a highway interdiction site.



Officers attending Pipeline schools are instructed to identify and articulate, both in spoken and written form, "specific indicators" that, when viewed collectively, give the officer reasonable suspicion that a motorist has violated the law. EPIC conducts between 20 and 25 Pipeline schools each year at no charge to the police departments.

Under the Operation Jetway program, EPIC also offers a more limited schedule of similar on-site instruction for officers involved in interdiction at airports, bus stations, train terminals, and commercial package services. The instruction program is similar to that of the Pipeline schools, with expanded emphasis on methods of concealment unique to packages and luggage.

To further enhance training opportunities for state and local agencies, EPIC allows free access to and use of its 140-seat conference center as a venue for training or other functions for the law enforcement community. The conference center has state-of-the-art audiovisual and computer capabilities and can accommodate sensitive and classified-subject presentations.

Standard Operating Procedure

EPIC has taken to heart the timeless adage that "all the information in the world is useless unless you get it to someone that can use it." Getting the right information to the right person at the right time is standard operating procedure. The kind of information that the center can provide to police departments leads to important seizures and arrests that ultimately prevent drugs from getting into the hands of Americans and drug money from getting into the hands of traffickers. From Maine to Miami, San Diego to Seattle and anywhere in between, EPIC is a resource that no department can afford to ignore.

Note: This article was originally published in the 6 June 2007 edition of *Police Chief Magazine*, Vol. 74.

Section 3: The Coast Guard and Homeland Security

Team of Teams: All-Hazard Incident Response Operations Call for U.S. Military Emergency Preparedness Liaisons

Commanders Martha LaGuardia-Kotite and David L. Teska, U.S. Coast Guard Reserve

"The 'team of teams' partners during a disaster, creating a synergy of agencies, which in turn sends a message of reassurance to the American people."—Lieutenant General H. Steven Blum, Deputy Combatant Commander, United States Northern Command

Haiti, January 2010

On 12 Jan. 2010 the earth beneath the Caribbean island nation of Haiti heaved and shook and the world responded. Its proximity to Haiti meant United States aid would come within days. Soon military and civilian responders from the United States were on the ground in Haiti providing humanitarian relief and searching the rubble of Port-au-Prince for survivors. In the following days and weeks more responders from across the region and from as far away as France, Belgium, the Netherlands, Canada, and Israel would arrive to render expertise and assistance to a battered people.

The Federal Emergency Management Agency (FEMA) leads the federal incident response effort when disasters occur in the United States or its territories and coordinates response operations across all levels of government. However, when the United States responds to a foreign disaster as it did in Haiti, the U.S. Agency for International Development (USAID), an agency of the U.S. Department of State, assumes the lead for the U.S. response in close coordination with the affected nation. Unlike U.S. disaster response operations governed by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), response efforts in Haiti required the United States and other foreign responders to work with the Haitian government, ever mindful of a sovereign nation's legal authority over its own internal affairs.

The United States quickly emerged as the primary provider of foreign assistance and the coordinator of foreign disaster relief to a shocked nation of 9 million people. Under the apt name Operation Unified Response, the United States dispatched a robust multiagency response effort coordinated by USAID that included the Department of Defense's (DOD's) Joint Task Force–Haiti out of U.S. Southern Command and the U.S. Coast Guard.

The U.S. Coast Guard has long operated in the waters around Haiti. Under federal law, the United States treats Cubans who defect as political refugees if they make it to U.S. soil. Haitians migrants, on the other hand, get repatriated to Haiti. Despite the U.S. policy, the political turmoil in Haiti since the early 1990s has resulted in on-again, off-again surges in boatloads of Haitians fleeing their nation for better opportunities in the United States The Coast Guard has been at the forefront of the effort to stem that flow. Frequently these efforts take on a humanitarian focus as many of the Haitian boats stopped are unseaworthy, woefully overloaded, and bereft of safety equipment, food, and water. Thus when the ground shook the Coast Guard was the first U.S. agency outside of Haiti to respond; the Coast Guard Cutter *Forward* (WMEC-911) arrived in Port-au-Prince on Jan. 13. *Forward* supported the relief effort for over a month before returning to its homeport in Portsmouth, Virginia in mid-February.[1]

Figure 1. PORT-AU-PRINCE, Haiti—Coast Guard Capt. John Little conducts a port coordination meeting while working diligently with other agencies to provide aid to Haitian earthquake survivors, 1 Feb. 2010.

The Coast Guard, a component of the U.S. Department of Homeland Security (DHS) since the department's creation in March 2003, quickly became a key player in the earthquake relief effort, easily leveraging its multimission capability. Port facilities in Port-au-Prince sustained tremendous damage (in fact, much of the port was in need of repair prior to the earthquake) and relief flights quickly overwhelmed the nation's major airport. The Coast Guard deployed an 11-person marine transportation system recovery unit (MTSRU) to assess the port and make recommendations to Haitian officials on the port's status and what it would take to restore the port's cargo handling capability. Coupled with assessing the port was the need to coordinate the flow of relief cargo ships converging on Haiti from around the world. The port's aids to navigation system needed repair and needed it quickly. The Coast Guard Cutter *Oak* (WLB-211), a sea-going buoy tender, left Charleston, South Carolina bound for Port-au-Prince to provide not only needed repairs but humanitarian relief efforts as well. A medical team from the cutter assisted other medical teams in Killick, Haiti. Additionally, the MTSRU operated a vessel traffic system from *Oak* that coordinated, in close conjunction with Haiti port officials, the flow of cargo ships in Haiti. Finally, as with most disasters, security of responders, of survivors, and of the port itself required attention. Members of Coast Guard Port Security Unit 307, an all-reserve unit which normally deploys overseas to provide shore-side and water-side port security when the United States conducts military cargo operations, performed the same mission in Port-au-Prince, ensuring that relief supplies arrived unimpeded. Coast Guard helicopters ferried badly injured Haitians to USNS *Comfort* (T-AH-20), the massive white-hulled hospital ship known around the world (along with its west coast sister ship, USNS *Mercy* (T-AH-19)). Coast Guard C-130s flew flights from air stations in south Florida to Haiti importing relief supplies and evacuating the injured to the United States for medical treatment.

Figure 2. PORT-AU-PRINCE, Haiti—U.S. Naval hospital ship, USNS *Comfort,* provides a platform for a U.S. Coast Guard HH-60 Jayhawk helicopter during a medical evacuation after a magnitude 7.0 earthquake destroyed much of Haiti's capital city, 20 Jan. 2010. U.S. Coast Guard photo by Petty Officer 3rd Class Brandon Blackwell.

Response efforts undertaken by the Coast Guard in the aftermath of the earthquake in Haiti are typical for a service able to marshal its resources and provide a wide range of assistance beyond what is typically tasked or expected. The Coast Guard has a long and storied heritage in disaster response since its inception in 1790 as the U.S. Revenue Cutter Service. Over the years the Coast Guard has expanded its mission set and emerged as a service well versed in providing a wide range of capabilities after a disaster. The assistance chronicled above is only a glimpse of the response capabilities the Coast Guard has at its disposal for use during disaster events. Another resource that characteristically works behind the scenes coordinates Coast Guard support to disaster-affected states and communities and to the federal responders assisting them. The U.S. Coast Guard emergency preparedness liaison officer (EPLO) team consists of a dozen seasoned Coast Guard reserve officers in designated billets who serve as forward sensors and provide early warning or situational awareness for unscheduled and scheduled events requiring civil support across America.

Team of Teams

At the annual national EPLO conference held in March 2009 in Henderson, Nevada, Lieutenant. General H. Steven Blum, Deputy Combatant Commander for United States Northern Command (USNORTHCOM), in his keynote address to service members, said the "team of teams" is a partnership that creates a synergy among agencies, which in turn "sends a message of reassurance to the American people." General Blum pointed out his support for the dedicated

men and women in the program, saying they also provide insights into the political intent of the people who are to be supported. As a "multipurpose sensor" the EPLOs can engage with state and elected officials before a federal request for military assistance. By attending state hurricane exercises, regional interagency steering committee (RISC) meetings, and response planning conferences, EPLOs make contacts, swap business cards, and become familiar with the people and agencies they may later support.

Small in numbers but strong in scope, this influential and resourceful team of men and women continue to fashion the Coast Guard's growing EPLO program into an impressive cadre of joint, interagency, and intergovernmental liaisons for disaster responses and events of national significance. The broad canvas of these events includes local incidents, such as floods and wildfires; catastrophic disasters with national effects to infrastructure, populations, and the economy, such as hurricanes or earthquakes; and national special security events (NSSE), including Republican and Democratic national conventions and Presidential inaugurations.

Coast Guard EPLOs are liaison officers dedicated to regional, state, and other emergency response organizations that coordinate federal response under the National Response Framework, the nation's all-hazard response guide.[2] EPLOs deploy to one of FEMA's 10 regional response coordination centers (RRCCs), disaster joint field offices (JFOs), and, on occasion, to a state or local emergency operations center (EOC) to provide liaison and coordination of Coast Guard support as directed by FEMA to either the affected states or to other federal partners involved in the disaster response efforts. But how is this multiagency response coordinated with the state and other federal agencies when an incident exceeds a state's ability to respond? Legal authorities are spelled out in a large library of federal laws and regulations including the Stafford Act, which states that the President can, "direct any federal agency, with or without reimbursement, to utilize its authorities and the resources granted to it under federal law (including personnel, equipment, supplies, facilities, and managerial, technical, and advisory services) in support of state and local assistance response and recovery efforts, including precautionary evacuations."[3]

When a disaster requires a military response to augment the state and other federal agencies, Coast Guard EPLO's coordinate with the "team of teams." This robust team includes U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine EPLOs; regional U.S. Army defense coordinating officers (DCOs) and defense coordinating elements (DCEs); FEMA regions; federal and state agencies (including the National Guard); and other partners including volunteer and church groups. Member teams rally as trusted agents at ground zero by alerting, staging, and deploying resources anywhere in America to answer the call for help and provide civil support to the states and American citizens. It is important to note the distinction between what DOD provides under defense support of civil authorities (DSCA) and the Coast Guard's disaster operations support, which does not fall under the umbrella of DSCA. This subtle but significant difference sets the Coast Guard's disaster response apart from DOD's DSCA mission.

As a whole, EPLOs from all military services are relatively unknown outside the interagency preparedness and response circles in which they serve. The Coast Guard EPLO program officially began in 2006. Within a relatively short time, the Coast Guard employed EPLO skills and service capabilities to complement the "team of teams" and engage in disaster responses or events of national significance. The DOD EPLO program began in the 1970s. Today, the DOD program is a robust organization of more than 400 EPLOs assigned to work with all FEMA regions and with the states.

Because Coast Guard EPLOs are reservists, they often provide invaluable professional knowledge gained from their civilian career experiences, which may prove helpful when responding to disasters. Reservists in this program, when not drilling or on active duty, are professionals in a variety of industries and professions, including government (federal, state, and local), law, medicine, security, information technology, public relations, and other fields.

Coast Guard EPLOs arrive with unique capabilities and authorities that enable their service to deploy and employ forces before the military components within DOD deploy. The Coast Guard has a distinctive blend of military, humanitarian, and law enforcement capabilities and fulfills a significant role as a federal first response agency, operating with local partners and supporting local authorities. The Coast Guard further solidified its EPLO program with the release of Commandant Instruction (COMDTINST) 3025.1, *USCG Emergency Preparedness Liaison Officer (EPLO) Program,* in September 2009. This document now serves as guidance for the Coast Guard EPLO Program. Among its provisions, COMDTINST 3025.1 stipulates that each of FEMA's 10 regions will have a reserve EPLO assigned and that Coast Guard EPLOs "maintain contact and intercommunication between elements of the Coast Guard and partner agencies."[4]

An example of this unique, joint capability occurred in March 2009 in North Dakota when the Red River of the North rose to record levels. As a result, the governor declared a flood emergency across the state. Flooding progressed as the river overran Fargo, North Dakota's largest city of 90,000 residents. The Coast Guard brought in resources from far and wide to render assistance and save more than 100 lives. When flood waters surged and moved north toward Canada, the Coast Guard's emergency responders moved with it. The Coast Guard teamed with the U.S. Fish and Wildlife Service, Customs and Border Protection, FEMA, the U.S. Army Corps of Engineers, the National Guard, DOD, and numerous other agencies and volunteers to assist North Dakota.

Figure 3. An HH-65 Dolphin helicopter from Coast Guard Air Station Traverse City, Mich., flies over the flooded Red River. Another Dolphin helicopter, from Air Station New Orleans, accompanied it during the transit from Grand Forks to Fargo to stand by for rescue operations, 28 Mar. 2009. U.S. Coast Guard photo by Petty Officer 3rd Class Erik Swanson.

Captain Charles Polk, U.S. Coast Guard Reserve (USCGR) officer, serves in his civilian occupation as an assistant federal security director with the U.S. Transportation Security Administration (TSA) in Little Rock, Arkansas. As a reservist, he was one of the first liaisons on scene in Bismarck when he was called away from TSA for nearly a week and deployed as the senior Coast Guard officer assigned to the state-federal JFO to help with the federal response to the Red River flood. The Coast Guard deployed four disaster assistance response teams (DARTs), shallow-draft boat teams used to rescue people from flooded structures; six HH-65C Dolphin helicopters from Air Stations Detroit, Traverse City, Sacramento, and New Orleans for search and rescue; and seven air boats. In addition to serving as the senior Coast Guard officer at the disaster's JFO, Captain Polk served as the lead for Emergency Support Function 9 (search and rescue) and as the Coast Guard "air boss," coordinating Coast Guard aviation assets providing search-and-rescue assistance to the citizens of Fargo and the surrounding area. "Lots of time directing what proved to be a very capable and hard-working staff," he said. "Overall, a great experience for an officer who had never been remotely close to either of the Dakotas."

Captain Polk's disaster assignment placed him among a cadre of reserve officers in the 8th Coast Guard District, which extends geographically from the Gulf of Mexico north through the Midwest states to the Canadian border. He and the other district liaisons volunteer to serve on a roster of available officers deployable to disaster response locations on behalf of the Coast Guard, providing needed expertise and service knowledge to federal and state emergency managers on the capabilities and limitations of Coast Guard response resources. While not officially assigned as EPLOs, liaisons like Captain Polk give the 8th District a badly needed capability to put eyes on the ground during a disaster's early phases.

In the waning days of August 2008, Commander David Teska, USCGR, received a call from the 8th Coast Guard District in New Orleans. The district command center had been monitoring hurricane Gustav's predicted track, which was now five days away from making landfall along the Gulf Coast. This powerful storm seriously threatened the vulnerable city of New Orleans, a serious issue for area residents with memories of Hurricane Katrina still very fresh. The 8th Coast Guard District asked Commander Teska to quickly deploy to the JFO, located in a converted Dillard's department store in Baton Rouge.[5] Within three days Commander Teska had packed his gear, said goodbye to his family in Lawrence, Kansas, and left his job working as the FEMA regional continuity planner in Kansas City, Missouri. He set up at the Louisiana JFO working to coordinate Coast Guard response operations in the immediate aftermath of Hurricane Gustav's landfall. During the seven days he deployed to the JFO, Commander Teska worked to provide mission-essential Coast Guard aviation support, a part of the service's overall response. The Coast Guard flew search-and-rescue missions soon after the hurricane-force winds subsided to around sixty knots. Then crews provided levee over-flights for the U.S. Army Corps of Engineers.

In addition to supporting missions with small boats and first responders on the ground, the Coast Guard also flew in support of the mission needs of the U.S. Department of Energy by providing aerial inspection trips of Louisiana's oil production infrastructure. The mission included checking the economically critical Louisiana Offshore Oil Port, or LOOP, where tankers dock and offload valuable oil cargo without needing to transit up the Mississippi River.

But Coast Guard EPLOs don't just deploy in advance of a hurricane's landfall or when rivers flood. They also provide support to the U.S. Secret Service, which is the lead agency for declared NSSEs. For Commander Richard McLaughlin, USCGR, deployment meant duty in our nation's capital assisting with the coordination of DOD and Coast Guard support for the inauguration of President Barack Obama in January 2009. Before the inauguration, Commander McLaughlin

served a key role as a maritime domain duty officer assigned to Joint Task Force Headquarters–National Capital Region (JTF–NCR). JTF–NCR serves as the military headquarters for land-based homeland defense, defense support to civil authorities, and incident management in the national capital region.[6] The sheer complexity and magnitude of the Presidential Inauguration, coupled with its unique security challenges, made it a top priority for Coast Guard and DOD EPLOs.

Distinct from short-fuse events like the funeral for former President Gerald R. Ford held in January 2007, most NSSEs are planned well in advance and allow the luxury of extensive and detailed planning and rehearsals. "This advance notice not only provides significant time for planning, training, and logistics coordination, it also allows time for our forces to prepare to deploy. This might include requesting time off from their employers and making travel and lodging plans," Commander McLaughlin said. "Providing support for a natural or man-made disaster is much more challenging since it requires an immediate response with little to no warning of the time, location or type of event."

Commander McLaughlin served as the Coast Guard liaison to an active duty colonel assigned to FEMA Region III as the DCO. The U.S. Army has assigned a DCO, supported by a DCE to every FEMA region. The DCO/DCE teams serve as a single point of contact for the deployment and employment of DOD forces when requested by FEMA. The DCO/DCE teams are under the command and control of U.S. Army North (ARNORTH),[7] the land component of USNORTHCOM at Ft. Sam Houston, Texas.

Even though the designation of officers to serve in the Coast Guard EPLO program is comparably recent, the men and women of the Coast Guard have proven essential to the nation's disaster response missions for 219 years. Seemingly, mainstream America truly became aware of them during the aftermath of Hurricane Katrina's devastation of Mississippi and Louisiana in August 2005. Yet these missions are not new and have long been familiar to those who live and work on the seas and waterways. The service's history of life-saving responses to the nation goes almost as far back as its inception. In the aftermath of the tragic sinking of *RMS Titanic*, Congress passed S.2337 in 1914—which President Woodrow Wilson signed into law on 20 Jan. 1915—creating the modern U.S. Coast Guard by merging the Revenue Cutter Service and the Life-Saving Service.[8] The Lighthouse Service would join the Coast Guard in 1939.[9]

As the multimission maritime service within DHS and one of the nation's five armed services, the Coast Guard's primary roles include protecting the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including international waters and America's coasts, ports, and inland waterways. Resources are applied towards performing in 11 mission areas: marine safety; search and rescue; drug interdiction; migrant interdiction; defense readiness; port, waterways, and coastal security; stewardship of living marine resources; marine environmental protection; fisheries law enforcement; aids to navigation; and ice operations.[10] Current operations in Iraq have seen the Coast Guard deploy personnel and resources in theater, again to apply their skills and expertise where needed.

Coast Guard EPLOs are Different

"What the Coast Guard is able to do and what it does in support of civil authorities, capabilities and mission requirements is determined by the needs of the specific event or scenario and always based on consultation with local, state and federal agencies," wrote Coast Guard Commandant Admiral Thad W. Allen in his *iCommandant* Web Journal.[11] DOD has a similar program, albeit

much larger, with a regional emergency preparedness liaison officer (REPLO) and REPLO team assigned to each of FEMA's 10 regional officers and a similar team of state emergency preparedness liaison officers (SEPLO) assigned to state emergency management agencies. In a major presidential disaster declaration, FEMA may call upon DOD to deploy forces to assist affected states; if this occurs the FEMA federal coordinating officer will turn to the DOD DCO to coordinate the assignment and deployment of DOD forces to that state at the direction of FEMA. Before requesting federal or DOD resources, the states also have access to an intrastate disaster assistance program. The Emergency Management Assistance Compact (EMAC) provides intrastate mutual aid during disasters. Under EMAC, the requesting state pays deployment costs (typically partially reimbursed by FEMA under disaster declaration). EMAC has proven highly successful and states make good use of it when the situation warrants a bigger response than the affected state can manage.[12]

Coast Guard EPLOs come to a disaster representing a service that is unique in many ways. The service is a federal agency with missions that it regularly conducts under its own statutory authority. First responders are typically local and not federally sourced, but the Coast Guard often deploys or prestages—for instance in the case of hurricanes—so that its resources are immediately available when needed most. Because of that authority and first responder posture, Coast Guard resources typically respond to a disaster under the service's own statutory authority, such as 14 U.S.C. § 89, the section of the U.S. Code that gives the Coast Guard its law enforcement authority.

Deploying Title 10 DOD resources, such as a Navy construction battalion or an Air Force Reserve expeditionary medical system (EMED), requires a FEMA-issued mission assignment with state concurrence for payment of 25 percent of the mission's costs. FEMA does mission-assign the Coast Guard, such as when conducting search and rescue in urban areas like New Orleans in the days after Katrina, but extenuating circumstances (like operating in a nontraditional area or performing a mission it normally doesn't perform) must exist. Conducting search and rescue in an urban environment is outside normal Coast Guard search-and-rescue jurisdiction, so a FEMA mission assignment is appropriate. The EPLO plays a key role in this process by serving as the service's subject-matter expert to FEMA and other agencies on Coast Guard resources, advising what they can do, cannot do, and should not do. All this is done in close coordination with the respective Coast Guard district overseeing the Coast Guard's response to the event.

Legal Issues: Posse Comitatus Act

DOD has enormous capability to provide resources to an affected state in the aftermath of a disaster, but there are legal restrictions that limit the range of DOD's response. One of the more obscure and often misunderstood is the Posse Comitatus Act (PCA). Citizen complaints surrounding the use of federal troops to enforce local laws in the states of the former Confederacy during Reconstruction (1865–1877) and questionable electioneering practices during the Presidential election of 1876 led Congress to pass the PCA in 1878. Specifically, the PCA states:

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.—18 U.S.C. § 1385.

For DOD, the PCA prohibits the use of the Army, Air Force, Navy, and Marine Corps to enforce federal, state, or local laws. Whereas DOD can provide logistical, medical, engineering, and other humanitarian assistance, it cannot deploy military forces (Title 10) to provide law enforcement support short of a declaration of the Insurrection Act or Martial Law.[13] This restriction includes the National Guard when under federal control (Title 10 status), which states clearly that "the Army National Guard while in the service of the United States is a component of the Army."[14] The PCA also applies to the Coast Guard only when "operating under the command and control of the Department of Defense."[15]

So, when does the PCA not apply? It does not apply to the National Guard when in Title 32 status or when employed on state active duty[16] (SAD) and it does not apply to the U.S. Coast Guard in most situations.[17] Unlike the National Guard, which loses law enforcement authority as prescribed by the PCA when activated under Title 10, the Coast Guard retains the law enforcement authority granted it under 14 U.S.C. § 89, even when activated under Title 10. Thus its unique status as an armed service with law enforcement authorities makes it a viable and flexible military and law enforcement agency.

The historical record of the use of Title 10 forces in domestic law enforcement is a brief one, as the PCA intended. The prime example unfolded in April 1992 in the aftermath of the Rodney King beating acquittal, when riots broke out across Los Angeles. The city, unable to quell the violence, requested state assistance. Governor Pete Wilson activated units of the California National Guard (under SAD), but more assistance was needed. On 1 May, President George H.W. Bush signed Executive Order 12804, evoking the Insurrection Act, federalizing select units of the California National Guard, and authorizing the use of active U.S. Army and Marine Corps units to assist in the restoration of law and order under the Operation Garden Plot plan.[18] A total of 10,000 Guardsmen, 1,500 Marines, and 2,000 Soldiers operated under the command and control of Joint Task Force–Los Angeles until their release on 6 May.[19] Only once has martial law existed in U.S. history: following the attack on Pearl Harbor on 7 Dec. 1941, martial law went into effect for the Territory of Hawaii and lasted nearly three years.[20]

The legal authority for the Coast Guard's disaster response operations "stems both from the Coast Guard's authority to conduct search and rescue and our ability to provide assistance to other federal, state and local agencies when our personnel are especially qualified to do so," Admiral Allen wrote in his *iCommandant* Web journal. This relevance is provided by 14 U.S.C. § 89 while 14 U.S.C. § 141 provides that "the Coast Guard, upon request, may use its personnel and facilities to assist any federal agency, state, territory, possession, or political subdivision to perform activities for which the Coast Guard is 'especially qualified'." While rendering assistance to flooded regions, the Coast Guard was able to provide assistance on the water because of the authorities given by 14 U.S.C. § 89, which authorizes the Coast Guard to board vessels subject to the jurisdiction or operation of any United States law on the high seas or on waters of U.S. jurisdiction. Additionally, Coast Guard Captains of the Port have "extensive authority to control the anchorage and movement of vessels, [and] establish safety and security zones in U.S. ports and waters subject to U.S. jurisdiction…." According to an article in the 03-09 issue of *USCG Reservist* magazine "the Coast Guard restricted boat traffic on more than 200 miles of the Red River due to the flooding. A safety zone was established between Wahpeton, in southeastern North Dakota, and Pembina on the U.S.-Canadian border." A broad spectrum of Coast Guard authorities are found within other U.S.C. sections, including the grant of law enforcement authority for shore-side investigations and law enforcement activities under 14 U.S.C. § 95 and limited law enforcement activities for Coast Guard personnel ashore at maritime facilities under 46 U.S.C. § 70118.

What this means to our DOD and state partners in emergency management is this: there are options for Coast Guard support to civil authorities beyond the usual maritime safety, security, and search-and-rescue operations. These operations, which are available in addition to normal mission requirements and cannot be sustained without additional support, include:

- Command and control (C2), which provides qualified personnel and deployable and mobile equipment support such as the DARTs and air boats deployed for the North Dakota flooding.
- Technical support for law enforcement, which includes bomb and drug detection equipment and canine teams.
- Air operations to augment and assist with surveillance, transportation, airlift and logistical support.
- Intelligence collection and analysis with the use of Coast Guard Investigative Service special agents.

All EPLOs have this in common: they are senior reserve officers who bring years of experience and service expertise which enable them to consult with state, local and federal partners and tailor the situation at hand with appropriate resources. With a coordinated and predesignated "team of teams," the nation is better prepared to effectively respond to all hazards: to incidents during a scheduled event, or to an unscheduled disaster. In 2008, the Coast Guard adopted its Guardian Ethos. Admiral Allen, in putting forward the Ethos, said that it "defines the essence of the Coast Guard," and is the "contract the Coast Guard and its members make with the nation and its citizens." The Ethos states, in part: "*I serve the citizens of the United States. I will protect them. I will defend them. I will save them. I am their shield. For them I am Semper Paratus*"[21] The Coast Guard's EPLOs strive to personify the heart of the Guardian Ethos by being *Semper Paratus*—always ready—to respond when needed and to live and serve as the American public has come to expect.

Commander LaGuardia-Kotite, author of the award winning book So Others May Live: Coast Guard Rescue Swimmers Saving Lives, Defying Death, has over 20 years of experience in the U.S. Coast Guard including 10 on active duty following graduation from the U.S. Coast Guard Academy. After serving as one of the Coast Guard's first EPLOs, she is now the Commandant's Press Secretary and in June returns to her assignment as senior reserve officer for Coast Guard Sector Mobile, Ala. Her next book, Changing the Rules of Engagement: Inspiring Stories of Courage and Vision from Military Women, will be released in 2011.

Commander Teska is a 1990 graduate of Officer Candidate School and is the Coast Guard EPLO to FEMA Region VII in Kansas City. He mobilized in January 2010 to Washington, DC in support of the Haiti earthquake relief efforts, and in 2008 he deployed to Baton Rouge for Hurricane Gustav. He has over 26 years of active and reserve military service in the U.S. Coast Guard and U.S. Army.

Note: The views expressed herein are those of the authors and are not to be construed as official or reflecting the views of the Commandant or of the U. S. Coast Guard or the Department of Homeland Security.

End Notes

1. Coast Guard Cutter *Forward* returns from Haiti, *PilotOnline,* 19 Feb. 2010, <http://hamptonroads.com/2010/02/coast-guard-cutter-forward-returns-haiti>, accessed 19 Feb. 2010.

2. Visit <http://www.fema.gov/emergency/nrf/aboutNRF.htm> for more on the National Response Framework.

3. Typically, federal agencies tasked by FEMA during a Stafford Act disaster do receive reimbursement under a process called Mission Assignments whereby FEMA directs a federal agency to provide assistance and then reimburses the agency for resource costs such as flight time and crew costs for aviation support.

4. USCG *Emergency Preparedness Liaison Officer (EPLO) Program,* COMDTINST 3025.1, paragraph 7-6-1., p. 9.

5. At the time, Coast Guard EPLO billets were assigned to the Coast Guard's office of incident management and preparedness (CG-533). They have since been re-assigned to the districts as outlined in COMDTINST 3025.1.

6. JTF–NCR homepage, <http://www.jfhqncr.northcom.mil/Mission/mission_main.html>, accessed on 19 May 2009.

7. U.S. 5th Army officially changed its name to ARNORTH in recognition of its role as the Army's lead in homeland defense and DSCA.

8. A third agency, the U.S. Bureau of Marine Inspection, permanently came under the Coast Guard on 16 Jul. 1946, Office of the Coast Guard Historian, <http://www.uscg.mil/history/faqs/when.asp>, accessed on 19 May 2009.

9. Office of the Coast Guard Historian, <http://www.uscg.mil/history/faqs/when.asp>, accessed on 19 May 2009.

10. Coast Guard Publication 1, *U.S. Coast Guard: America's Maritime Guardian,* Washington, D.C., May 2009, pp. 5-11.

11. Coast Guard Support to Civil Authorities, *iCommandant:* Web Journal of Admiral Thad Allen, <http://www.uscg.mil/comdt/blog/archive/2009_03_01_archive.asp>, accessed on 29 Jul. 2009.

12. Visit <http://www.emacweb.org/> for more information on EMAC.

13. DODD 5525.5 prohibits "direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law." *Domestic Operational Law (DOPLAW) Handbook for Judge Advocates*, Vol. 1, 2006, Center for Law and Military Operations, p. 16.

14. Title 10 Armed Forces, Subtitle E, Reserve Components, Sec. 10106, <http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=BROWSE&TITLE=10USCSE>, accessed 24 Feb. 2010.

15. *DOPLAW Handbook,* p. 16.

16. The National Guard operates either in Title 32 status, such as during monthly drills and when on active duty for training (ADT), state active duty, as when called up by a state or territorial governor for disaster response, or Title 10, when called up by Congress or mobilized by the President to support national security such as the current conflicts in Iraq and Afghanistan. For an excellent explanation of the National Guard's legal statuses, see *DOPLAW Handbook*, Ch. 10, pgs. 195.201.

17. *Operational Law Handbook*, The Judge Advocate General's Legal Center & School, Charlottesville, Va., 2008, pg. 198-199.

18. *DOPLAW Handbook*, Chapter 4, Section E, The Department of Defense Civil Disturbance Plan (Operation Garden Plot), pg. 77-93.

19. Operation Garden Plot: JTF–LA Joint Task Force–Los Angeles, *Global Security.*, <http://www.globalsecurity.org/military/ops/jtf-la.htm>, accessed on 19 Feb. 2010.

20. Martial Law Held Sway in Isles for Three Years, *The Honolulu Star-Bulletin*, <http://archives.starbulletin.com/1999/09/13/special/story5.html>, accessed on 19 Feb. 2010.

21. ALCOAST 366/08, *The Guardian Ethos*, <http://www.uscg.mil/announcements/alcoast/ALCOAST36608.txt>, accessed on 2 Aug. 2009.

Customs and Border Protection, Coast Guard, and Immigration and Customs Enforcement Senior Guidance Team: Improving the unity of effort within Department of Homeland Security

Captain Tony Regalbuto (USCG, Ret.) and Mr. Michael Perron

Reprinted with permission from *Proceedings.*

In June 2006, ADM Thad Allen, Commandant of the U.S. Coast Guard (USCG), and Mr. Ralph Basham, Commissioner of Customs and Border Protection (CBP), chartered a senior guidance team (SGT) represented by flag officers and senior executives from both agencies to improve our near-and long-term efficiency and effectiveness. ADM Allen and Mr. Basham indicated that CBP and the USCG were committed to a "one team, one fight" approach to our nation's security, whereby improving our efficiency and effectiveness will provide greater results for our nation.

Customs and Border Protection and the Coast Guard have played significant roles not only during the early formative years of the United States,[1] but throughout our nation's history. However, the threats of asymmetrical attacks have provided greater visibility to our agencies and more focus on and scrutiny of our missions. As ADM Allen has said in numerous forums following the September 11 terrorist attacks, "We (the Coast Guard) have never been more relevant, and we have never been more visible to the nation we serve." Clearly, the same could be said for Customs and Border Protection.

CBP and the USCG are two prominent law enforcement agencies in the Department of Homeland Security (DHS) with field presence in our ports of entry, between ports of entry (land and maritime borders), in coastal areas, in high seas, and in our international trade partners' ports. Both agencies also have broad statutory authorities, robust capabilities, and missions that are necessary for our nation's security. Therefore it is incumbent upon CBP and the USCG to work efficiently and effectively to better prepare our nation to prevent, protect, respond to, and recover from terrorist attacks, natural disasters, and other incidents of national significance.

Initial Focus

In one of the first meetings of the senior guidance team, the leaders highlighted that there were three things that Customs and Border Protection and the Coast Guard needed to focus on, namely:

1. We need to better understand our dramatically changed operating environment.

2. We must change to sustain and improve our mission execution.

3. We must be more responsive to the needs of the nation.

As co-chairs for their respective agencies, Mr. Jayson Ahern, CBP Deputy Commissioner, and VADM David Pekoske, then USCG Deputy Commandant for Operations, quickly established ground rules for the senior guidance team. They agreed to meet quarterly and to form joint working groups to improve the efficiency and effectiveness of agency operations.

Initially the co-chairs formed work groups in:

- Small vessel strategy to better address the small vessel threat;
- Joint operation centers to improve command and control and information sharing;
- Joint boardings for better mission execution;
- Resumption of trade so the nation could recover from any hazard including terrorist attacks and hurricanes.

Ongoing Strategy

Building on the successes of the initial work, the co-chairs recently formed additional workgroups in:

- Joint unmanned aircraft to build capability for DHS and its component agencies;
- Joint training to improve the interoperability of agency assets;
- Joint vessel targets are intercepted, interrogated, and apprehended or neutralized, if necessary;
- Joint logistics to improve the support to our people and assets at a reduced cost;
- Joint budget development to better source the agencies based upon a joint strategy;
- Joint specialized forces to improve interoperability of specialized forces in response to a hazard.

In January 2008 the co-chairs invited Immigration and Customs Enforcement (ICE) to the senior guidance team meeting. Since then, ICE has been an active participant in the quarterly meetings and has gained valuable insight in the workgroup initiatives to date. In April 2008, the chairs decided to form a new workgroup on mass migration to better address processing migrants after they have been interdicted.

The Small Vessel Strategy Working Group

The small vessel[2] environment is an area of significant concern, and is particularly vulnerable to exploitation by terrorists, smugglers, and other criminals. When attempting to address this risk, law enforcement personnel must be able to distinguish the relatively few individuals engaged in illicit activities among the vast number of legitimate vessel operators. The challenge is immense, involving more than 17 million registered U.S. recreational vessels, 82,000 fishing vessels, and 100,000 other commercial small vessels. Also, law enforcement agencies have very little operational awareness of these small vessels, which makes the sorting even more challenging.

To address this risk, the senior guidance team chartered a small vessel strategy working group in December 2006. In preparation for a DHS-sponsored National Small Vessel Security Summit, held in Washington, D.C., in June 2007, the team directed the working group to develop small

vessel strategic principles. The working group developed the principles to address the broad framework needed to close some of the gaps and vulnerabilities that small vessels presented and to help shape the discussion with the stakeholders at the summit.

The DHS National Small Vessel Security Summit report was released by DHS Secretary Chertoff in January 2008. Based upon requests for more engagement from the small vessel stakeholders at the national summit, regional summits were held in Cleveland, Ohio; Orlando, Fla.; Long Beach, Calif.; and Cape Cod, Mass.

These provided more dialogue and feedback among DHS, its component agencies, and the small vessel stakeholders.

Following the summit, Secretary Chertoff directed the DHS Small Vessel Security Component Agency Working Group to take the recommendations of the stakeholders and findings from the summit and develop a DHS Small Vessel Security Strategy. Secretary Chertoff released the final strategy to the public at the American Boating Congress Legislative Conference held in Washington, D.C., in April 2008. The workgroup will also develop an implementation plan that will provide a roadmap of specific actions DHS will take to reduce the risk of small vessels.[3]

Joint Operations Center Working Group

Several recent presidential directives charged DHS to provide seamless, coordinated implementation of authorities and responsibilities relating to the security of the maritime domain by and among federal departments and agencies. Additionally, Section 108 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) directed that interagency operations centers be established at all high-priority ports.

The SGT recognized that DHS component agencies must work together at field levels to implement these strategies. This would promote a unity of effort for maritime planning and operations. The team also recognized that joint operations centers would provide the command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities to ensure proper maritime domain awareness and to lead and manage operations. The SGT established the Joint Operations Centers Working Group to provide greater capability for CBP/USCG field units.

The Coast Guard's established Interagency Operations Centers/Command 21 (IOC/C21) Initiative (renamed from Command 2010) will provide capabilities to increase maritime domain awareness, automate data gathering, and provide a decision support capability that captures the actions and processes of the watch. To support the SAFE Port Act, IOC/C21 will also provide facilities to support the information sharing necessary to coordinate federal, state, and local port partner activities in the conduct of daily joint operations; sensors to establish enterprise radar and camera coverage throughout the port; and information management systems (called Watch-Keeper) to link information with operations to support decision making, situation awareness, joint planning, and mission execution.

IOC/C21 is the maritime component of the DHS Secure Border Initiative. The SGT agreed that implementing the acquisition of these major systems fell beyond the scope of this working group. However, the SGT directed the workgroup to take an active role in ensuring the necessary lash-up between the Secure Border Initiative and IOC/C21 project staffs to ensure good governance.

The workgroup also identified seven pilot port projects to review, hone best practices from, and evaluate various types of coordination models used (in-person, virtual, 24/7, and co-location of CBP/USCG units). Those ports where in-person coordination has been prototyped include Seattle, Charleston, and Detroit. Virtual coordination has been prototyped in New York and Tampa/St.Petersburg. Coordination using 24/7 CBP watch standers in the USCG command center has been prototyped in San Diego. The USCG and CBP have developed a planning proposal to collocate field units in Jacksonville.

A follow-on survey conducted in early 2008 revealed much greater interagency coordination, with notable increases in intelligence sharing (23%), joint vessel targeting (27%), coordinated patrolling (23%), and joint daily ops briefings (10%) from the previous year. The ports of Jacksonville, Tampa/St. Petersburg, and Charleston were also cited as being among the national leaders for demonstrating exceptional interagency coordination.

Joint Boardings Working Group

This working group focused on expanding joint CBP and USCG boardings to improve mission execution at the field level, and reduce the burden of potential multiple boardings on the maritime industry.

In October and December 2005, Customs and Border Protection and Coast Guard personnel participated in conferences to share the results of collaborative efforts, best practices, and obstacles they had to overcome to create a more effective working environment. They identified five overarching dual-agency law enforcement activities to improve mission execution, including vessel targeting, dual-agency boardings, information sharing, training, and professional exchanges.

As a follow-on, the workgroup directed implementation of the five joint CBP/USCG enforcement activities and directed development of local standard operating procedures to institutionalize and formalize these processes. CBP directors and USCG captains of the port were required to prepare joint quarterly status reports highlighting their successes in these five areas.

The first reports indicated they were achieving great success in terms of opening up the lines of communication, developing positive working relationships, increasing joint boardings and training, and developing officer exchange programs. The July 2007 reports highlighted that co-location of resources had been achieved by several field units, and standard operating procedures development, daily interagency briefings, joint targeting and boardings, and information sharing protocols had increased considerably nationwide.

To improve training, the Coast Guard's Maritime Law Enforcement Academy and CBP's Federal Law Enforcement Training Center partnered to consolidate curriculum from existing weapons of mass destruction courses. Staff developed a combined course and began training CBP and USCG field personnel beginning in the spring of 2008.

Field units began conducting joint training in law enforcement authorities; boarding team tactics, techniques, and procedures; use of force; standardized personal protective equipment; confined space entry; hazardous materials; and fraudulent document identification.

To provide stakeholder awareness and gain feedback, leaders from the working group met with the Commercial Operations Advisory Committee, National Maritime Security Advisory Committee, and the Maritime Security Coordinating Committee. These industry groups provided positive feedback and additional recommendations on boarding practices and training. For example, an industry representative recommended that a panel of industry members speak to law enforcement officers in training so they can better understand the industry's needs and concerns.

As a result of the joint targeting initiatives at the field level, the SGT stood up a separate Joint Targeting Working Group in January 2008 to identify best practices in targeting processes and potential areas for more collaboration and analysis at the national level.

Building upon the success of the joint boarding program afloat, the workgroup began focusing its attention on pierside boardings and inspections to identify opportunities to expand CBP/USCG cooperation. The group established pilot programs at the USCG sectors and CBP field offices in

Seattle, Washington and Jacksonville, Florida. Subsequently, vessel agents and operators in these ports expressed the concern that joint pierside boardings and/or inspections are difficult for the ships to manage due to dissimilarities between the CBP and USCG focus. They indicated their preference to have sequential examinations to ease the burden on the vessel's crew. Based upon this feedback, the pilot ports began exploring the feasibility of one agency conducting business on behalf of the other, rather than joint activities.

However, the joint boardings have already proved to be safer, smoother, and more effective operations. They are continuing to provide more substantial enforcement results and improve overall situation awareness. Results include the identification and repatriation of numerous stowaways, seizure of containers due to trademark violations, seizure of contraband such as shark fin and narcotics, and several arrests.

Resumption of Maritime Trade Working Group

As far back as 2002, the Maritime Transportation Security Act required that the National Maritime Transportation Security Plan include a plan to restore cargo flow following a national transportation security incident. This concept again surfaced in Homeland Security Presidential Directive 13 and the National Strategy for Maritime Security. Subsequently, strategic concepts supporting efficient marine transportation system (MTS) recovery following a transportation security incident were documented in the Maritime Infrastructure Recovery Plan. Shortly thereafter, the lessons learned from Hurricane Katrina also widely acknowledged that MTS disruptions can result in significant economic ramifications, and the U.S. must be prepared to execute efficient and effective MTS recovery management to minimize these negative effects. Most recently, the SAFE Port Act of 2006, Section 202, required that protocols for the resumption of trade be developed by July 2007.

The Coast Guard hosted a national maritime recovery symposium in August 2006 to further explore the issues and potential alternative solutions regarding developing robust MTS recovery and resumption of maritime trade capability. The symposium participants, executives from both government and industry, identified the need for:

- specific procedures and protocols to execute recovery/resumption strategies;
- integration of government and private sector efforts and mechanisms for communication and information sharing among government and private sector stakeholders during recovery management;
- underlying systems of information and prioritization tools to support recovery management decision making.

Both the USCG and CBP have equities, responsibilities, and authorities that are brought to bear following a significant MTS disruption, and specifically following a maritime transportation security incident. The SGT recognized that the USCG and CBP must work together to develop and implement the necessary protocols and recovery management procedures to ensure the most efficient resumption of trade flow following a MTS disruption. Timely development of these protocols was also necessary to meet the requirements outlined in Section 202 of the SAFE Port Act.

The working group reviewed a draft strategy to enhance the security of the international supply chain and incorporated comments regarding resumption of trade principles. Group members then drafted CBP/USCG joint protocols for the expeditious recovery of trade and held discussions with components of the Departments of Homeland Security, Transportation, and Defense to explain the process and seek input. The protocols were signed by Commissioner Basham and USCG ADM Allen in the spring of 2008 and distributed to the public and maritime stakeholders.

The goals of the protocols are to:

- Establish a communications process at the national level to be employed by the USCG, CBP, other federal agencies, and the maritime industry following or prior to an event causing a major disruption to the MTS.
- Consider the collateral impacts of a major disruption of the MTS on international commerce. Support federal decision making and protection of federal interests.
- Establish how the USCG and CBP will interact with other government agencies to jointly facilitate the expeditious recovery of the national MTS and resumption of commerce, including Maritime Infrastructure Recovery Plan-related activities.
- Support National Security Presidential Directive-41/Homeland Security Presidential Directive-13 and the protection of the national economy and national defense.
- Support the SAFE Port Act mandate to develop protocols for the resumption of trade in the event of a transportation disruption.

As part of this effort, the Coast Guard worked with the Maritime Administration to create a port capability inventory of the 150 largest U.S. ports. This inventory will be used to inform national decision makers about port system capabilities. The USCG also drafted a Commandant

Instruction that provides guidance to field units on including recovery in their area maritime security plans and creating recovery units within their incident command system. CBP also developed a Web-based messaging system to alert the trade community of significant disruption in trade flow in all modes of international transportation. CBP will coordinate each maritime message with the USCG to ensure the alignment of a unified DHS response.

About the authors

Captain Tony Regalbuto (USCG, Ret.) is a 1971 graduate of the State University of New York's Maritime College, earning a bachelor of science degree in meteorology and oceanography. He served on active duty for the Coast Guard for 31 years and was the acting port security director following the September 11 terrorist attacks. In his civilian capacity, he is currently serving as chief of the Office of International and Domestic Port Security Assessments.

Mr. Michael Perron graduated magna cum laude from California State University, Dominguez Hills, earning a bachelor of arts degree in political science, with a minor in communications. He served on active duty with the U.S. Army for 10 years as a military police sergeant and a Criminal Investigation Division special agent. He has been employed by U.S. Customs and Border Protection (formerly the U.S. Customs Service) for the past 21 years, including assignments as chief inspector, enforcement in Los Angeles and port director, Washington, D.C. He is currently assigned to CBP headquarters as the acting associate director for Deliberate Planning.

End Notes

1. Responding to the urgent need for revenue, President George Washington signed the Tariff Act of July 4, 1789, which authorized the collection of duties on imported goods. It was called "the second Declaration of Independence" by the news media of that era. On July 31, 1789, the fifth act of Congress established the U.S. Customs Service and its ports of entry to collect the revenues. The United States Coast Guard, one of the country's five armed services, traces its history back to August 4, 1790, when the first Congress authorized the construction of 10 vessels to enforce tariff and trade laws, prevent smuggling, and protect the collection of the federal revenue.

2. Small vessels are characterized as any watercraft less than 300 gross tons, regardless of method of propulsion. Small vessels can include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other commercial vessels involved in foreign or U.S. voyages.

3. The report of the DHS National Small Vessel Security Summit and the DHS Small Vessel Security Strategy can be reviewed or downloaded at www.dhs.gov.

Note: This article was originally published in the spring 2009 edition of *Proceedings.*

Coast Guard Boosting Cooperation with Military

Matthew Rusling

Reprinted with permission from *National Defense.*

Last summer, as Russian forces lay siege to the nation of Georgia, the Coast Guard cutter Dallas, along with two Navy ships, sailed to the Black Sea to provide relief. The Coast Guard crew, under Operation Assured Delivery, docked at the port of Bat'umi, and delivered 80 pallets of humanitarian assistance supplies.

There are likely to be more joint missions such as these for the Coast Guard, officials said. The Dallas, prior to the Georgia mission, participated in Africa Partnership Station, an initiative to improve maritime safety and security in West and Central Africa.

The Coast Guard's traditional role has been to undertake missions off U.S. shores—"the home game"—while the Navy has usually worked overseas—"the away game." But the Coast Guard has officially incorporated into its doctrine the idea of further integration with other military branches. And it is increasingly putting this idea into practice.

In October 2007, the Navy, Marine Corps and Coast Guard released a joint document, entitled "A Cooperative Strategy for 21st Century Seapower," which outlines this new doctrine of cooperation. "Coast Guard forces must be able to operate as part of a joint task force thousands of miles from our shores," a pamphlet describing the document said. "And naval forces must be able to respond to operational tasking close to home when necessary to secure our nation and support civil authorities."

"It's the first time in history, at least that we found documented, that the commandant of the Marine Corps, the commandant of the Coast Guard and the chief of naval operations signed a joint document that began to define how [they]…will work with each other," said Rear Adm. Jody Breckenridge, director of the Coast Guard's strategic transformation team. She spoke at the annual National Defense Industrial Association's Coast Guard conference and exhibition. The challenge for the Coast Guard will be to implement those ideas, she said.

"I think the biggest [challenge] is operationalizing the joint maritime strategy that the Marine Corps, the Coast Guard and the Navy have signed. That is going to be the way forward," she said.

In line with the new doctrine, the service will increasingly act in places where the Navy might not. This could include places where sending a Navy ship overseas, even to deliver aid, could give the wrong political message, said Dana Goward, director of Coast Guard assessment, integration and risk management. Anchoring a naval vessel off another country's shores could be perceived as threatening, he said. The cutter Dallas that helped to deliver relief supplies to Georgia is one example.

"In many instances a Coast Guard boat is much more acceptable to a foreign nation because it is not from the [Defense Department]," Goward said. These types of missions will increase, he added. "When natural or manmade disasters strike, our maritime forces can provide humanitarian assistance and relief, joining with interagency and nongovernmental partners," the joint document said.

The vast majority of the world's population lives within a few hundred miles of the ocean, the document noted. "Social instability in increasingly crowded cities, many of which exist in already unstable parts of the world, has the potential to create significant disruptions. The effects of climate change may also amplify human suffering through catastrophic storms, loss of arable lands, and coastal flooding," the document said.

In response to these climate change concerns, the Coast Guard is also filling in a gap in the Arctic, where it operates the nation's fleet of polar icebreakers. Melting sea ice has made the region a potential hotspot as various nations lay claim to its waters and natural resources.

"That's a direct example of how we are a unique force provider for the [Defense Department] and the Navy," Goward said. "The Navy doesn't have any icebreakers there."

Coast Guard Commandant Adm. Thad Allen said cooperation between his service and the other branches is growing. He is speaking to the Navy about how to best integrate the use of unmanned aerial vehicles into the new National Security Cutters, which are designed to operate thousands of miles from U.S. shores. "Our intention is to be joint and to be closer," Allen said of the Navy and the Coast Guard.

The Navy is now allowing Coast Guard personnel to try out for its elite, special operations teams, the sea, air and land forces, commonly known as the SEALs. Those who make it through the two-year training program will be assigned to a SEAL team for five to seven years, although they will remain officially part of the Coast Guard.

The Coast Guard is unique among the armed forces because it operates in two worlds. As a law enforcement agency, its personnel can make arrests where their military counterparts are prohibited from doing so under the Posse Comitatus Act. "Frequently we will put law enforcement detachments aboard naval vessels.… That ship will fly the Coast Guard [flag] to show that it is now a law enforcement vessel," Goward said. If that boat encounters any illegal activity, it can take action, he added.

The two branches have also conducted joint exercises. More than 930 Navy and Coast Guard active-duty and reserve personnel participated in the maritime security operations exercise Seahawk in the summer of 2007. The exercise's goal was to boost interoperability, officials said. It focused on preventing violent extremists from using the sea as a route for attacks on land.

The Coast Guard also maintains a joint training center at the Marine Corps base in Camp Lejeune, N.C. The Coast Guard's Special Missions Training Center offers courses, teaches doctrine and conducts testing and evaluation of equipment.

The program is a part of an effort to provide standardized port security training for Navy, Coast Guard and Marine Corps personnel. Coast Guard courses range from basic skills in securing ports to lessons in pursuing non-compliant vessels. Marine Corps classes include small boat unit leadership. Navy courses give instruction in such subjects as combat and interdicting small craft.

As the Coast Guard aims for closer partnerships with the rest of the military, the question arises of whether true jointness is feasible. Cooperation entails precise planning and careful coordination. But Allen said relations between the branches of the military are good and that he expects integration to improve.

Note: This article was originally published in the Jan. 2009 edition of *National Defense*.

One Small Boat Among Many Can Be a Big Problem

Edward H. Lundquist

Reprinted with permission from Faircount Media Group and *Coast Guard Outlook.*

The damaged USS Cole (DDG 67) is towed away from the port city of Aden, Yemen, into open sea by the Military Sealift Command ocean-going tug USNS Catawba (T-ATF 168) on Oct. 29, 2000. Cole was placed aboard the Norwegian heavy transport ship M/V Blue Marlin and transported back to the United States for repair. The Arleigh Burke-class destroyer was the target of a terrorist attack in the port of Aden Oct. 12, 2000, during a scheduled refueling. The tragic attack killed 17 crewmembers and injured 39 others. DoD photo by Sgt. Don L. Maes, U.S. Marine Corps

A small boat comes alongside the USS *Cole*, moored at Aden, Yemen, and explodes. The October 2000 terrorist attack killed 17 U.S. sailors and injured 39 more.

The terrorists who attacked the French supertanker *Limburg* in October 2002 did so in a small boat packed with explosives.

The Lashkar-e-Taiba terrorists, who struck Mumbai in November 2008, killing 166 people over three days, came by sea in a hijacked fishing boat.

In April 2004, three dhows packed with explosives approached the vital Iraqi Khawr al Amaya Oil Terminal in the northern Arabian Gulf when one was approached and boarded by U.S. sailors and Coast Guard personnel from the USS *Firebolt*. The dhow exploded, killing two sailors and a Coast Guardsman.

During the long-running conflict in Sri Lanka, terrorists have frequently employed small boats to smuggle terrorists and weapons to the island and for attacks on commercial and military vessels.

In each of these incidents, the watercraft involved looked just like many other small pleasure craft or commercial vessels common to their area of the world. The overwhelming majority of pleasure craft and small commercial vessel operators are responsible and law-abiding. But an innocuous, small vessel has tremendous potential to deliver dangerous people, be built into a bomb, or deliver a weapon of mass destruction (WMD).

"If you consider what a small boat did to the USS *Cole*, then you can understand why I say there is nothing that worries me more than a waterborne improvised explosive device in one of our ports," said Adm. Thad W. Allen, commandant of the Coast Guard.

Large vessels certainly have the potential to be involved in a serious security breach, but these ships are registered, regulated, inspected, and tracked. Their voyages are planned and their movements monitored by the Coast Guard. However, the sheer number of smaller pleasure craft or commercial vessels – less than 300 tons – represent a different and more pressing challenge. While there are about 80,000 ships of more than 300 tons operating in some capacity today around the world, there are nearly 13 million registered recreational vessels and another 8 million non-registered recreational vessels in the United States alone, along with another 80,000 fishing vessels and thousands of other commercial vessels. These small vessels may operate near or next to large container ships, cruise liners, chemical tankers, or warships, as well as critical infrastructure facilities ranging from power plants and refineries to bridges and building. With 95,000 miles of coastline to monitor, it's a daunting challenge if one of those vessels among the many means to cause harm.

For terrorists seeking to kill innocent people, cripple U.S. infrastructure, or just get their story told, this maritime environment provides tempting opportunities. While authorities are not warning of such an impending attack, the prudent thing to do is to reduce the nation's vulnerability in the maritime domain. "We don't want to wait for another attack to take action," Allen said.

The gravest maritime threat facing the nation is the potential for a terrorist group to obtain a nuclear weapon or other WMD and use it within the confines of a major U.S. port. The "Coast Guard Strategy for Maritime Safety, Security, and Stewardship" states, "While much focus has been placed on WMD detection in maritime containers, it is equally probable, if not even more likely, that such a device would be loaded onboard a low-value bulk freighter, a fishing boat, or a recreational yacht or power boat that allows constant possession of a WMD device by a terrorist group. Many of these vessels also operate under minimal regimes and protocols for control, making their movements mostly anonymous to authorities. The catastrophic impacts of such a terrorist attack, launched within dense urban port areas, make this a particularly lethal threat."

While most large vessels are registered and tracked, small untracked vessels pose a huge threat because of the possibility of operating near or even close aboard container ships to offload improvised explosive devices within U.S. ports and waterways. There are some 13 million registered recreational vessels and another 8 million non-registered recreational boats in the United States alone. U.S. Coast Guard photo by PA3 Barbara L. Patton

Vigilance is an all-hands effort. The Coast Guard must closely coordinate its efforts with other federal, state, and local agencies, as well as local boaters and marinas.

"We rely on the people who live and work here, the way a community relies on a neighborhood watch," said Capt. Leon Nixon, chief of the Port of Los Angeles Police Department. "We call it the 'Harbor Watch.' We visit the bait piers and talk to the fishermen. We hear from the residents who live aboard their boats who live in marinas. They'll tell us if something doesn't look right."

If a vessel looks suspicious, or is in the wrong place, authorities do not need permission to board or search. Where the Coast Guard can board any vessel to conduct safety inspections, the Port of Los Angeles Police Department has the authority to ensure local ordinances are being enforced. Where appropriate, the Port of Los Angeles Police and the Coast Guard work together to conduct inspections.

The port is home to the CGC *George Cobb*, from which personnel can also report on unusual activity when servicing aids to navigation in and around the port.

In addition to working very closely with the Coast Guard, Nixon said his agency works with the Port of Long Beach, the Los Angeles County Sheriff's Department, the Los Angeles and Long Beach police departments, Los Angeles City and County Life Guards, the Los Angeles Fire Department, the Federal Bureau of Investigation, Customs and Border Protection, and the Port of Los Angeles Pilots. "It's a one-team approach. It's all very cohesive here."

It's a huge challenge to keep track of all the big ships on our oceans and rivers. But it's an even bigger challenge to maintain an appropriate awareness of the numerous small vessels in American waters. For example, Florida has more registered motor vessels than any other state, with approximately 988,000 registered recreational boats. Since the majority of small vessel operators are professional mariners or legitimate recreational boaters, the Coast Guard strives to develop strong partnerships with the people most familiar with their local environment.

The Coast Guard's America's Waterway Watch (AWW) is a partnership involving the Coast Guard, the Coast Guard Auxiliary, and commercial, municipal, and recreational organizations across the nation. AWW seeks to raise the collective consciousness of those engaging in a multitude of waterborne activities to stay alert for the potential of encountering suspicious or unusual activities on the U.S. waterways. The AWW Web site (http:// americaswaterwaywatch.uscg.mil) contains information and material that can help people understand how they can contribute by knowing what constitutes suspicious behavior and how to promptly report it. AWW has proven critical to assisting the Coast Guard and other law enforcement agencies in their efforts to sustain the nation's maritime security.

Through AWW, everyone can feel ownership for the security of America's waterways. Those who routinely work or recreate on any particular waterway are the ones most likely to be the best sources for identifying suspicious or unusual activity. Such "local knowledge" helps the Coast Guard and other law enforcement organizations to best leverage limited manpower and resources. "The backbone of America's Waterway Watch is its partners and participants, without which AWW couldn't fulfill its commitment to maritime safety and security," said Lt. Cmdr. Jim Rocco. "They're exceedingly vital to sustaining the nation's safety and security vigilance."

"A call to 1-877-24WATCH provides direct communication to the national call center for the Department of Homeland Security [DHS], which will start the ball rolling to have suspicious concerns monitored and investigated," he said.

A U.S. Coast Guard boat and a Georgia Department of Natural Resource boat patrol the east side of Elba Island on the Savannah River in front of the liquefied natural gas facility. Critical structures around the nation are potential sites for would-be terrorists. As a deterrent, the Coast Guard's America's Waterway Watch has proven to be a successful program, receiving assistance by other law enforcement agencies, as well as the public – all of whom look for and report unusual activities. U.S. Coast Guard photo by PA2 Dana Warr

One such call came in March 2003: A suspected terrorist with connections to al Qaeda was arrested after telling an undercover FBI agent of his interest in buying enough plastic explosives "to blow up a mountain." Another came under scrutiny when he asked a local tour boat captain how close a boat could approach local bridges and cruise ships. The captain promptly notified the Coast Guard via AWW.

Operation Focused Lens (OFL) is a Coast Guard-led anti-terrorism operation in California ports and waterways. As a best practice, it incorporates aspects of both security operations and maritime domain awareness (MDA) and has tie-ins with AWW. While building trust with the public, this operation directs field units to perform focused and coordinated air, land, and sea surveillance patrols, small vessel security boardings, and intelligence collection activities in areas where small boat attacks or boat bombs may originate, be staged, or executed. OFL employs risk and predictive analytics for resource allocation and is tasked with targeting those areas most likely to be used as a staging area for such an attack. Its activities deter and prevent terrorists from exploiting marinas, boat ramps, and similar areas from which to stage attacks. Operations are conducted in partnership with other DHS and local law enforcement agencies, Coast Guard Auxiliary, and the boating public, and leverages AWW. During fiscal year 2009, Coast Guard units in California held 630 AWW events where 4,565 boaters learned about suspicious incident reporting. Additionally, 2,401 security boardings occurred in and around marinas and 7,343 surveillance patrols were conducted, of which more than 700 were performed by local law enforcement. These activities greatly assisted the Coast Guard's efforts to build MDA, presence, and trust in areas not previously visited by law enforcement.

In 2008, DHS released its comprehensive Small Vessel Security Strategy (SVSS) after obtaining citizen input. The SVSS addresses the four scenarios of gravest concern involving terrorist attacks using small vessels: (1) use as a waterborne improvised explosive device; (2) smuggling weapons (including WMDs) into the U.S.; (3) smuggling terrorists into the U.S.; and (4) as a platform for conducting a stand-off attack (e.g., Man-Portable Air Defense System or a ballistic missile). The Coast Guard-led interagency team has developed the Small Vessel Security Implementation Plan, which lays out the federal, state, tribal, and local actions required to achieve the goals and objectives of the SVSS. The implementation plan has been drafted and is being concurrently reviewed at department and national levels for approval and release in early 2010.

A coherent strategy, deliberate execution, and broad stakeholder involvement are critical to deterring or interdicting terrorist small boat attacks in the United States.

Capt. Edward H. Lundquist, USN (Ret.), is a senior science advisor with Alion Science and Technology in Washington, D.C.

Note: This article was originally published in the 2010 edition of *Coast Guard Outlook*.

Section 4: Protecting Our Cyber Borders

Cyberspace and the "First Battle" in 21st Century War

Robert A. Miller and Daniel T. Kuehl

Reprinted with permission from *Defense Horizons.*

Overview

Wars often start well before main forces engage. In the 19th and early 20th centuries, combat often began when light cavalry units crossed the border. For most of the 20th century, the "first battle" typically involved dawn surprise attacks, usually delivered by air forces.[1] While a few of these attacks were so shattering that they essentially decided the outcome of the struggle or at least dramatically shaped its course—the Israeli air force's attack at the opening of the June 1967 Six-Day War comes to mind—in most cases the defender had sufficient strategic space—geographic and/or temporal—to recover and eventually redress the strategic balance to emerge victorious. The opening moments of World War II for Russia and the United States provide two examples.

The first battle in the 21st century, however, may well be in cyberspace.[2] Coordinated cyber attacks designed to shape the larger battlespace and influence a wide range of forces and levers of power may become the key feature of the next war. Early forms of this may have already been seen in Estonia and Georgia. Control of cyberspace may thus be as decisive in the network-dependent early 21st century as control of the air was for most of the 20th century.

In the future, cyber attacks may be combined with other means to inflict paralyzing damage to a nation's critical infrastructure as well as psychological operations designed to create fear, uncertainty, and doubt, a concept we refer to as *infrastructure and information operations*. The cyber sphere itself is, of course, a critical warfighting domain that hosts countless information infrastructures, but the rise of network-based control systems in areas as diverse as the power grid and logistics has widened the threat posed by network attacks on opposing infrastructures.

Given the increasing dependence of the U.S. military and society on critical infrastructures, this cyber-based first battle is one that we cannot afford to lose. And yet we might.

First Battles in American History

Historically, time and space to recover have often proven essential in overcoming losses in an opening battle. The United States frequently has fared poorly in the opening battles of past conventional wars—the other side, usually authoritarian or totalitarian, spends more time preparing the initial blow. As Charles Heller and Bill Stofft point out in their classic study of America's first battles, there's a pattern here.[3] In many cases, especially those in which the United States was engaged with a technologically advanced peer competitor, our first engagements have been disastrous. Only because America had sufficient (sometimes barely sufficient) strategic space—geographic and/or temporal depth—were we able to recover from our first defeats.

World War II provides examples across all three of that war's operational domains and with several combatants in different theaters. At sea, our initial efforts at submarine and carrier warfare, which became indispensable components of our victory in the Pacific, were hesitant and

marked by faulty equipment, ineffective doctrine, and a steep learning curve for personnel.[4] In the air, we discovered that one of the keystones of our prewar airpower doctrine—the efficacy of unescorted precision strategic bombing—was sadly in error, and the lack of fighter escorts for our bombers in 1943 cost us hundreds of bombers and thousands of crewmen. It was not until 1944 that German exhaustion and the arrival of the P–51 gave us air superiority in Europe, without which the victories of 1944–1945 would have been simply impossible. On land, our initial encounters with the Wehrmacht went poorly, as shown by the disaster at Kasserine Pass and the difficulties encountered throughout the North African and Italian campaigns. Not until the advance across France in the summer of 1944 did our skill at conducting combined arms maneuver warfare begin to match that of our German adversary. In all three examples, the time gap between the opening failures and the eventual victories was measured in months to years.

Even today, as we have most recently seen in Iraq, it has taken time and many casualties to change course and implement a strategy based on what seems to be more effective counterinsurgency principles.

We have been lucky to have had the time, space, and resources to correct these early problems. The question we face now is whether our luck will continue to hold in different operational conditions of the cyber age. Will that all-important time gap between early defeats and final victory be there for us now and in the future if we are faced with an enemy who is adept in and has planned for warfighting in the emerging fifth dimension of cyberspace, and who has avoided self-imposed and organizationally and programmatically based constraints on its operational concept for cyberspace operations?[5] The Chinese, for example, have been writing since the 1990s about the evolving "networked and informationized" battlefield, and one gains a clear sense that their approach to cyberwarfare is different than U.S. concepts.

Evolving Threats

Twentieth-century warfare was dominated by mass struggles of so-called conventional forces, created and sustained by the productive power of the industrial state and shadowed by the specter of weapons of mass destruction. The mushroom cloud and carpet bombing were its symbols, set-piece battles between symmetrically conceived forces its hallmark.

These 20th-century images have not yet left us, but they have been joined by new apparitions. The most visible, of course, is the kind of struggle that U.S. forces now find themselves fighting in Iraq and Afghanistan. Half war and half pacification campaign, these fierce struggles would once have been called "low intensity conflicts" or (more distantly) "irregular campaigns." No longer.[6]

But while our attention has been fixed on the conflicts in the Middle East, a different kind of national security threat has also emerged in recent years.

Military forces since time immemorial have tried to confuse their enemies and disrupt their plans, cut their communications, and throw them off balance.[7] However, the advent of the cyber age has changed things in some significant ways. Two factors increase the stakes of the cyber struggle. Tactically and operationally, the increasing dependence of modern technologically advanced forces (especially U.S. forces) on networks and information systems create new kinds of exploitable vulnerabilities. Second, as modern societies—including the militaries that mirror them—have continued to evolve, they have become ever more dependent on a series of interconnected, increasingly vulnerable "critical infrastructures" for their effective functioning.

These infrastructures not only have significantly increased the day-to-day efficiency of almost every part of our society, but they have also introduced new kinds of vulnerabilities. The increasing exposure of nations such as the United States to well-coordinated attacks on critical infrastructures creates a situation that we have labeled "strategic fragility."[8] The evolution of Russian strategic thinking throughout the 1980s and 1990s incorporated the potential to degrade national economic systems and communications networks as a means of breaking the enemy's will to resist and inflicting military and political defeat, at low cost and without the need to occupy territory.[9]

These interconnected and interdependent infrastructures represent new kinds of strategic targets. Take them down, and societies are effectively paralyzed. And yet successful action against them does not depend, as it once would have, on massive destruction of the physical infrastructure. In many cases, effective paralysis can be achieved by other cheaper and subtler means. In short, it is now possible to create chaos without carnage, disruption without destruction.[10]

"Weapons of Mass Disruption"

The chances of creating nondestructive chaos have been immeasurably increased by a second, related development—the increased dependence of the other infrastructures on the information infrastructure as a control mechanism. Most of the critical infrastructures that daily life relies on—electricity, communications, money, and transportation, to cite just four—now use cyberspace and the Internet to exchange information and directions. If this traffic, or the underlying data that are transmitted, is interrupted or tampered with, confusion and disorder will quickly break out.[11]

Attacks on the cyber infrastructure are one variant of what the military refers to as "information operations," and these attacks have been going on in one form or another for some years now.[12] So far, however, they have been in the nature of probes rather than strategic attacks designed to disable major infrastructures or affect the overall balance of military forces.[13] In the one case in which actual conflict included cyber activity—Russia's operations against Georgia in 2008—the Georgian infrastructure was simply not sufficiently sophisticated to be vulnerable to a cyber attack.[14]

We think that this is about to change.

The Opening Shot

It seems increasingly probable that the first battles in any future conflict involving technologically advanced adversaries will be electronic and waged in/via cyberspace.[15] Strategic cyber attacks will likely have multiple objectives:

- to disrupt enemy communications and supply lines
- to distract and confuse enemy command and control
- to impair the movement of military forces
- to create opportunities for strategic attacks on enemy infrastructures

- to deny similar capabilities to the enemy
- to weaken and distract social cohesion and political will, perhaps even before the conventional start of a conflict
- to shape global perceptions of the conflict.

First battle cyber attacks are likely to use a combination of approaches. These could include attempts to deny services critical to military capability, from logistics support to actual warfighting systems, and might include rapid, coordinated attacks to deny network connectivity. Attacks that deny data are the most obvious use of the new capabilities. Additionally, because of our heavy and growing dependence on what can be termed *dual-use infrastructures*—those owned and operated by the private sector that both society itself and military forces depend on for daily functioning of critical capabilities—the target of those attacks may not be prepared or resourced to withstand the kind of pressure that could be brought to bear by a coordinated and nation-state–sponsored series of attacks. A potential target list might include:[16]

- telecommunications
- space-based sensors and relays
- automated aids to financial and banking networks
- power production and distribution
- media to shape public perceptions.

In addition, we may also see attempts to manipulate the content of stored information through such means as injecting spurious information (attacks on data integrity). Modern military forces, and modern societies in general, rely on large databases of information that are essential for daily life and effective operations. If these databases become unreliable, the likely result is bedlam. So we should also expect to see attempts to reduce the adversary's confidence in the reliability of his networks and systems (attacks on confidentiality). As one senior Air Force leader observed at a symposium hosted at Air University in July 2008, the threat of data denial was much less worrisome than that of data manipulation.[17] Evidence of this threat extends as far back as Operation *Desert Shield*, the logistics and force deployment buildup to Operation *Desert Storm*, during which the intrusions into nearly three dozen American computer networks and databases by the so-called Dutch Hackers forced the delay of elements of the deployment because of the necessity to verify the contents of the databases that had been affected.

While the cyber events in Estonia (2007) and Georgia (2008) may not have reached the level of cyberwar, the targeted functions in both countries bore striking similarity to those listed above. In Estonia, effects were felt across the financial and media sectors; in Georgia, the cyber effects were also accompanied by an actual shooting war, although the less developed state of Georgia's use of cyberspace limited the cyber impact.[18]

Estonia 2007/Georgia 2008

The past two summers have seen examples of what the future may hold, albeit on a less developed scale. In the spring of 2007, the world witnessed what may have been the first major cyber-based assault on a nation-state, one that was perhaps particularly vulnerable because of

its heavy use of and dependence on cyberspace. Estonia, although a small and relatively lightly populated country (about 1.3 million, roughly the same as urban Stockholm, Sweden), is one of the most highly connected countries in the world; citizens often refer to their country as "eStonia." Both the public and private sectors are heavily dependent on cyberspace.

The details that caused the cyber incident are less important than what happened. To protest a perceived insult and injustice to Russia, someone launched a persistent but technologically simple distributed denial of service attack against a range of Estonian targets, coupled with some Web site defacements. Some were against the public sector (for example, Estonia's Parliament and Office of the President), while some were against key infrastructure elements in the private sector (banks, telecommunications, and media). The peak of the attacks came between May 4–8, 2007, but they did not present any technologically new features, and the largest ones presented all the signs of a botnet, whose use had been purchased for a limited and specified period of time. Estonian internal coordination and mitigation actions were successful in minimizing the impact of these assaults, and the perpetrators have never been identified. While the common belief is that the Russians did it, no one has ever been able to perform any digital forensics linking the attacks to the Russian government. Perhaps ethnic Russians who were displaying their anger using the new medium of cyberspace were to blame, but the only person formally charged with any offense was an Estonian.[19] While the incident prompted widespread and sometimes breathless "Cyberwarfare is Under Way!!" headlines, it had no impact on the Estonian military forces or national security apparatus. It was, however, a bit of a wakeup call.

That wakeup call was repeated even more loudly the following year, in August 2008, against the small country of Georgia, deep in the Caucasus region between Russia and Turkey/Iran to the south. But the differences between the Estonia situation and the one faced by Georgia were pronounced. Estonia is a heavily "wired" and connected society, whereas Georgia is at the opposite extreme.[20] The 2007 incident was completely cyber, except for some minor civil disturbances, and completely civilian, with no impact on Estonian military systems or sites. In Georgia, on the other hand, the cyber incidents went hand in hand with a significant conventional military operation by Russian forces, with rocket attacks into Georgian territory and an incursion by armored forces. Cyber actions against Georgian political leaders began well before the crisis blew up into military operations, with attacks on/defacement of Georgian President Mikheil Saakashvili's Web site 3 weeks before the start of combat operations. Because of Georgia's much lower use of (and thus lower dependence on) cyberspace for the control and use of key infrastructures, the cyber attacks conducted against Georgia concentrated primarily on blocking its ability to access the outside world and tell its side of the evolving story. Targets included President Saakashvili, the Foreign Ministry, and the Defense Ministry. Once again, claims that a second cyberwar was under way had to be measured against the unresolved question, "What is a cyberwar?"[21]

Both incidents raise a series of unanswered questions. What, for example, constitutes a sufficiently aggressive or damaging cyber event to involve the North Atlantic Treaty Organization? While most discussion has focused on Articles 4 (the need for consultation) and 5 (collective self defense against an "armed attack"), Article 6, which delineates what constitutes an "armed attack," seemingly limits that to actions against territory, forces, vessels, or aircraft. What are the limits and requirements for neutrality in cyberspace? Shortly after Russian tanks moved against Georgia and its governmental Web sites were defaced and taken over by unknown attackers, an ethnic Georgian expatriate in the United States who owned Tulip Systems in Atlanta began hosting the Georgian sites on Tulip servers. Since the legal status of the Russian-Georgian incident was unclear—was an "armed conflict" under way?—it cannot be firmly argued that Tulip violated any neutrality laws, but the question remains interesting.[22]

Information and Infrastructure Operations

In the 1990s, it became fashionable in American military circles to speak of a "revolution in military affairs," arising from a combination of technological breakthroughs, changes in the geopolitical balance due to the end of the Cold War and the collapse of the Soviet Union, and the growing conventional military superiority of the United States and its allies. As many theorists pointed out, all of these factors suggested that future conflicts—at least those involving U.S. forces—were likely to become "asymmetric," as others tried to figure out ways to counter U.S. predominance in conventional and nuclear military power.[23]

As we have seen in Iraq and Afghanistan—mirroring lessons learned from many previous insurgencies—lightly armed insurgents can have a considerable degree of success against conventional forces, especially if they use tools of the cyber age as force multipliers.

For the reasons discussed above, it seems likely that we are seeing the beginnings of a new kind of military operation, which could be referred to as information and infrastructure operations (I2O). I2O warfare could:

- combine with other types of operations
- be largely fought in cyberspace. Special operations and limited kinetic efforts directed at key infrastructure targets, single points of failure, and chokepoints are also likely.
- have strategic as well as operational/tactical goals
- offer important asymmetric advantages against a society/military dependent on networked systems and capabilities
- offer important advantages to the first mover. Combined with the relative ease of initiating such I2O, this provides powerful incentives to a hostile (or merely nervous) potential adversary to initiate actions.
- be limited through resilience strategies and, perhaps, be deterred by the development of retaliatory capabilities
- delay counter actions because of the inherent difficulty in obtaining high-confidence attribution of attacker identity
- drive other military forces to exploit cyber capabilities regardless of the United States doing so
- be decisive in achieving war aims.

Command and Control Issues

The U.S. Government, and particularly the military, has been paying increased attention to cyber threats in recent years.[24] As yet, however, much of this effort has seemed, at least from a distance, somehow dissociated from broader strategic and operational concerns—as if the cyber struggle will be confined to a series of "exploits" that will be pursued in their own realm with little contact with other events. In particular, the possibility of I2O as an element of a larger military and national security strategy has received little attention in the United States.

The Cyber Battle

We predict that in any future conflict, strategic infrastructures will be a major, and perhaps decisive, battleground, and I2O will be *the* critical set of operations in that battleground. We also expect that cyberspace will be the major theater for the conduct of such operations, if only because it offers a fast, relatively inexpensive, and effective way to assail and degrade critical but vulnerable infrastructures.[25]As a consequence, we also expect that the struggle for cyberspace dominance will be a difficult one, fought at the beginning of hostilities and probably begun long before. Since modern military operations have already become cyber dependent, and are rapidly increasing this dependence for operations and logistics, this cyber struggle for mastery will have significant consequences for a nation's ability to deploy, support, and fight, especially in a conflict of short duration aimed at focused and limited objectives. Winning that future *war*—defined in Clausewitzian terms as the attainment of strategic political objectives—thus may depend on successfully waging and winning the "first battle in cyberspace."

Dr. Robert A. Miller and Dr. Daniel T. Kuehl are Professors in the Information Resources Management College at the National Defense University. They can be reached at millerr@ndu.edu and kuehld@ndu.edu.

End Notes

1. Examples of the latter include the German attack on Poland in 1939, Japanese attack on Pearl Harbor, Israeli attack on Egypt at the start of the 1967 war, and coalition attack on Iraq in 1991, although the latter was a surprise only in a tactical sense.

2. This is obviously a hypothetical construct because the 21st-century's first battles have already been waged in Afghanistan and elsewhere.

3. Charles E. Heller and William A. Stofft, eds., *America's First Battles, 1776–1965* (Lawrence: University Press of Kansas, 1986).

4. This was also true for early operations in the Battle of the Atlantic, during which U.S. shipping was so badly ravaged by German U-boats that their crews called this period (early 1942) the "happy times." However, a significant cause of this was the stubborn refusal of senior U.S. Navy leadership, especially Admiral Ernest King, to adopt the convoy system, rather than an across-the-board problem.

5. The definition of *cyberspace* is still evolving. The Department of Defense uses the definition that originated with the Deputy Secretary of Defense in mid-2008 and has been codified into doctrine. *Cyberpower and National Security* (NDU Press and Potomac Books, 2009) offers a slightly different definition, emphasizing the role of the electromagnetic spectrum. The distinctions are more than merely semantic; how one defines an environment defines how one will use it.

6. This is at the heart of the growing debate over the future direction of U.S. military doctrine and force structure. Secretary of Defense Robert Gates seems to emphasize irregular warfare as seen in Iraq and Afghanistan, while his sharpest critics seem to emphasize the need to be ready to fight the "big war" against a near/peer nation-state competitor. If both eventualities must be guarded against, can we afford both force structures? One of the axioms of military preparedness is that the next war will almost assuredly not look like the last war. If this is true, basing our preparedness for the next war on the insurgency/counterinsurgency model could be disastrous.

7. If this sounds like the classic treatise on Chinese warfare by Sun Tzu, *The Art of War,* the resemblance is intentional. It also closely mirrors the Palestine Campaign waged by Field Marshal Edmund Allenby in 1918.

8. See Robert A. Miller and Irving Lachow, Defense Horizons 59, *Strategic Fragility: Infrastructure Protection and National Security in the Cyber Age* (Washington, DC: NDU Press, 2008).

9. Paul M. Joynal, "The Brave New World of the 5 Day War: Russia-Georgia Cyberwar, Where Cyber and Military Might Combined for War Fighting Advantage," available at <www.nationalstrategies.com/pdf/publicSafety_GovSec_5DayWar_Joyal.pdf>.

10. For a somewhat dated but still useful examination of non-U.S. concepts and capabilities, see Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States" (Hanover, NH: Institute for Security Technology Studies, November 2004), which examines six countries' capabilities, including Russia and China.

11. See Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Information Infrastructure Protection Policies* (Zurich: Centre for Security Studies, 2008). About every 2 years, this Swiss think tank publishes an extensive and thoroughly researched survey and analysis of national Critical Information Infrastructure Protection efforts. While each nation defines differently what constitutes a critical infrastructure, there are two that all 25 countries agree on: electricity and telecommunications.

12. See Joint Publication 3–13, *Joint Doctrine for Information Operations,* for definitions of the various "core competencies" included under the umbrella of information operations.

13. American practice distinguishes between computer network attacks and exploitation probes; the latter can be thought of as reconnaissance efforts looking for weak spots and trying for stray bits of useful information. Although the exact number, nature, and source of any of these efforts are classified, it is clear that their number and sophistication have steadily increased in recent years. As the U.S. military becomes more dependent on network-based operations, cyber attacks on it will inevitably become more attractive to others.

14. Eneken Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Learned," presentation at the NATO Cooperative Cyber Defence Centre of Excellence, August 2008.

15. Ibid. The timing of cyber actions, which occurred perhaps coincidentally with Russian military operations during the incursion into Georgia in the summer of 2008, suggests this possibility. Although Georgian military capability was in no way dependent on that nation's rather limited cyber-based infrastructures, Georgia's ability to inform the outside world of events there was certainly degraded.

16. Joynal.

17. This conference was hosted by Lieutenant General Robert Elder, then-commander of 8th Air Force, and included a panel led by Major General Bill Lord, then-commander of Air Force Cyber Command (Provisional).

18. For an interesting discussion of the Estonian and Georgian situations, as well as an exploration of a notional future cyberwar scenario, see Andrew F. Krepinevich, *Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York: Bantam Books, 2009), especially 232–237.

19. Analysis taken from Eneken Tikk, "Cyber Attacks: Estonian Lessons Learned," presentation at the George Mason University Critical Infrastructure Protection Project, 2008; and Tikk, "Legal Lessons Learned from the Georgia and Estonia Events," *Cyber Warfare 2009,* London.

20. While Estonia ranked 33d in the world in terms of Internet penetration with 57 percent, Georgia did not even register with only 8 percent penetration. See <www.internetworldstats.com/top25.htm>.

21. Tikk et al.; and Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008–2009).

22. Korns and Kastenberg.

23. This follows work done in the former Soviet Union in the 1980s on what had been termed the "military-technical revolution." Both seem to be responsible for much of the gene pool on which current concepts of "transformation" are based.

24. The Obama administration creation of a task force on cyber security is evidence that this issue has reached the highest levels of the U.S. Government. The publication in early 2009 of two Chatham House studies—one focusing on "Cyberspace and the National Security of the United Kingdom," the other on "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks," both edited by Paul Cornish—are evidence that the importance of this issue is recognized. Both reports are accessible at <www.chathamhouse.org.uk/research/security/>.

25. A series of recent major U.S. strategy and policy documents have referred to cyberspace as a "theater of operations" and part of the "global commons," reflective of the growing realization that cyberspace is and will continue to be a vital, perhaps decisive, environment for military operations.

Note: This article was originally published in the September 2009 edition of *Defense Horizons.*

Operate Effectively in Cyberspace

Reprinted with permission from *Quadrennial Defense Review.*

Our assessments of conflict scenarios involving state adversaries pointed to the need for improved capabilities to counter threats in cyberspace—a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks. Although it is a manmade domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.[1] There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.

It is therefore not surprising that DoD's information networks have become targets for adversaries who seek to blunt U.S. military operations. Indeed, these networks are infiltrated daily by a myriad of sources, ranging from small groups of individuals to some of the largest countries in the world. For example, criminals may try to access DoD's healthcare systems in order to obtain personal information to perpetrate identity theft. Terrorists may seek to disrupt military networks and systems to cause chaos and economic damage. Foreign intelligence or military services may attempt to alter data in DoD databases to hinder our military's ability to operate effectively. DoD must actively defend its networks.

This is no small task. DoD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DoD computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications. The number of potential vulnerabilities, therefore, is staggering. Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favor the offense. This advantage is growing as hacker tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication.

We must therefore be constantly vigilant and prepared to react nearly instantaneously if we are to effectively limit the damage that the most sophisticated types of attacks can inflict. In this environment, the need to develop strategies, policies, authorities, and capabilities for DoD to manage and defend its information networks is manifest. DoD is taking a number of steps to strengthen its capabilities in the cyberspace:

- **Develop a comprehensive approach to DoD operations in cyberspace.** A Department-wide comprehensive approach will help build an environment in which cyber security and the ability to operate effectively in cyberspace are viewed as priorities for DoD. Strategies and policies to improve cyber defense in depth, resiliency of networks, and surety of data and communication will allow DoD to continue to have confidence in its cyberspace operations. A central component of this approach is cultural and organizational: The Department will adapt and improve operational planning, its networks, its organizational structures, and its relationships with interagency, industry, and international partners. New operational concepts, such as dynamic network defense operations, could enhance effectiveness by enabling more rapid actions and more comprehensive actions to protect DoD's networks.

- **Develop greater cyberspace expertise and awareness.** The Department will redouble its efforts to imbue its personnel with a greater appreciation for the threats and vulnerabilities in the cyber domain and to give them the skills to counter those threats and reduce those vulnerabilities at the user and system administrator levels. DoD can no longer afford to have users think of its information technologies and networks as simply the benign infrastructure that facilitates their work. Users and managers must be held accountable for ensuring network security and for implementing best practices. DoD is also growing its cadre of cyber experts to protect and defend its information networks and is investing in and developing the latest technologies to enable our forces to operate in cyberspace under a wide range of conditions, including in contested and degraded environments.

- **Centralize command of cyberspace operations.** In an effort to organize and standardize cyber practices and operations more effectively, the Department is standing up U.S. Cyber Command (USCYBERCOM), a subunified command under U.S. Strategic Command, to lead, integrate and better coordinate the day-to-day defense, protection, and operation of DoD networks. USCYBERCOM will direct the operation and defense of DoD's information networks, and will prepare to, and when directed, conduct full spectrum cyberspace military operations. An operational USCYBERCOM will also play a leading role in helping to integrate cyber operations into operational and contingency planning. In addition, DoD is training cyber experts, equipped with the latest technologies, to protect and defend its information networks. Essential to the success of this new approach will be the capabilities and growth of the Service components that are stood up to support USCYBERCOM.

- **Enhance partnerships with other agencies and governments.** Freedom of operation in cyberspace is important and DoD must have the capabilities to defend its own networks. However, the interdependence of cyberspace means DoD networks are heavily dependent on commercial infrastructure. Just as it does in conducting many of our missions, DoD needs to collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense. In particular, DoD will strengthen its cooperation.

End Notes

1. The man-made nature of cyberspace distinguishes it from other domains in which the U.S. armed forces operate. The Administration will continue to explore the implications of cyberspace's unique attributes for policies regarding operations within it.

Note: This article was originally published in Feb. 2010 edition of *Quadrennial Defense Review.*

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL Web site. The CALL Web site is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

<http://call.army.mil>

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL home page: "Request for Information or a CALL Product" or "Give Us Your Feedback."

PROVIDE TACTICS, TECHNIQUES, AND PROCEDURES (TTP) OR SUBMIT AN AFTER ACTION REVIEW (AAR)

If your unit has identified lessons learned or TTP or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

NIPR e-mail address: call.rfimanager@conus.army.mil

SIPR e-mail address: call.rfiagent@conus.army.smil.mil

Mailing Address: Center for Army Lessons Learned, ATTN: OCC, 10 Meade Ave., Bldg 50, Fort Leavenworth, KS 66027-1350.

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at: <http://call.army.mil>. Use the "Request for Information or a CALL Product" link. Please fill in all the information, including your unit name and official military address. Please include building number and street for military posts.

PRODUCTS AVAILABE "ONLINE"

CENTER FOR ARMY LESSONS LEARNED

Access and download information from CALL's Web site. CALL also offers Web-based access to the CALL Archives. The CALL home page address is:

<http://call.army.mil>

CALL produces the following publications on a variety of subjects:

- **Combat Training Center Bulletins, Newsletters, and Trends**
- **Special Editions**
- ***News From the Front***
- **Training Techniques**
- **Handbooks**
- **Initial Impressions Reports**

You may request these publications by using the "Request for Information or a CALL Product" link on the CALL home page.

COMBINED ARMS CENTER (CAC)
Additional Publications and Resources

The CAC home page address is:

<http://usacac.army.mil/cac2/index.asp>

Battle Command Knowledge System (BCKS)

BCKS supports the online generation, application, management, and exploitation of Army knowledge to foster collaboration among Soldiers and units in order to share expertise and experience, facilitate leader development and intuitive decision making, and support the development of organizations and teams. Find BCKS at <http://usacac.army.mil/cac2/bcks/index.asp>.

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <http://usacac.army.mil/cac2/cal/index.asp>.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history. Find CSI products at <http://usacac.army.mil/cac2/csi/csipubs.asp>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <http://www.usapa.army.mil> or the Reimer Digital Library <http://www.adtdl.army.mil>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <http://fmso.leavenworth.army.mil/>.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <http://usacac.army.mil/cac2/militaryreview/index.asp>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA Threats at <https://dcsint-threats.leavenworth.army.mil/default.aspx> (requires AKO password and ID).

Combined Arms Center-Capability Development Integration Directorate (CAC-CDID)

CAC-CDIC is responsible for executing the capability development for a number of CAC proponent areas, such as Information Operations, Electronic Warfare, and Computer Network Operations, among others. CAC-CDID also teaches the Functional Area 30 (Information Operations) qualification course. Find CAC-CDID at <http://usacac.army.mil/cac2/cdid/index.asp>.

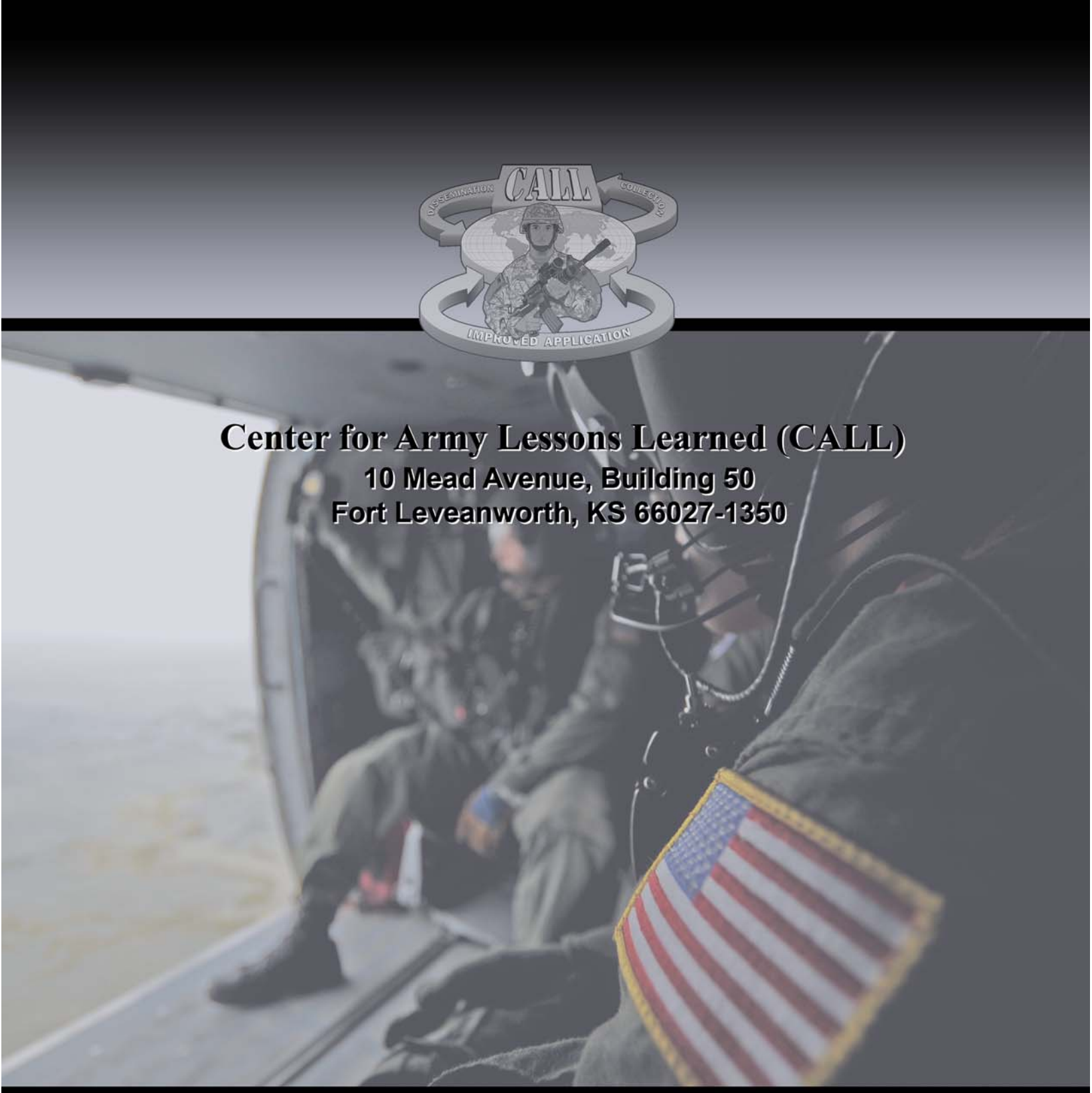
U.S. Army and Marine Corps Counterinsurgency (COIN) Center

The U.S. Army and Marine Corps COIN Center acts as an advocate and integrator for COIN programs throughout the combined, joint, and interagency arena. Find the U.S. Army/U.S. Marine Corps COIN Center at: <http://usacac.army.mil/cac2/coin/index.asp>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <https://jcisfa.jcs.mil/Public/Index.aspx>.\

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.



Center for Army Lessons Learned (CALL)

10 Mead Avenue, Building 50
Fort Leveanworth, KS 66027-1350

http://call.army.mil

US Army Combined Arms Center
"Intellectual Center of the Army"